

TRANSMITTAL LETTER TO THE UNITED STATES  
DESIGNATED/ELECTED OFFICE (DO/EO/US)  
CONCERNING A FILING UNDER 35 U.S.C. 371

ATTORNEY'S DOCKET NUMBER

KOIK-T0185

U.S. APPLICATION NO. (IF KNOWN, SEE 37 CFR 1.5)

09/647378

INTERNATIONAL APPLICATION NO.  
PCT/JP00/00904INTERNATIONAL FILING DATE  
17 February 2000 (17.02.00)PRIORITY DATE CLAIMED  
17 February 2000 (17.02.00)

TITLE OF INVENTION

INFORMATION PROCESSING APPARATUS AND METHOD, AND PROGRAM STORAGE MEDIUM

APPLICANT(S) FOR DO/EO/US

KAWAKAMI, Itaru; ISHIGURO, Ryuji; TANABE, Mitsuru and EZURA, Yuichi

Applicant herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information:

1. ☒ This is a **FIRST** submission of items concerning a filing under 35 U.S.C. 371.
2. ☐ This is a **SECOND** or **SUBSEQUENT** submission of items concerning a filing under 35 U.S.C. 371.
3. ☒ This is an express request to begin national examination procedures (35 U.S.C. 371(f)) at any time rather than delay examination until the expiration of the applicable time limit set in 35 U.S.C. 371(b) and PCT Articles 22 and 39(1).
4. ☐ A proper Demand for International Preliminary Examination was made by the 19th month from the earliest claimed priority date.
5. ☒ A copy of the International Application as filed (35 U.S.C. 371 (c) (2))
  - a. ☐ is transmitted herewith (required only if not transmitted by the International Bureau).
  - b. ☒ has been transmitted by the International Bureau.
  - c. ☐ is not required, as the application was filed in the United States Receiving Office (RO/US).
6. ☒ A translation of the International Application into English (35 U.S.C. 371(c)(2))
7. ☒ A copy of the International Search Report (PCT/ISA/210).
8. ☒ Amendments to the claims of the International Application under PCT Article 19 (35 U.S.C. 371 (c)(3))
  - a. ☐ are transmitted herewith (required only if not transmitted by the International Bureau).
  - b. ☒ have been transmitted by the International Bureau.
  - c. ☐ have not been made, however, the time limit for making such amendments has NOT expired.
  - d. ☐ have not been made and will not be made.
9. ☒ A translation of the amendments to the claims under PCT Article 19 (35 U.S.C. 371(c)(3)).
10. ☒ An oath or declaration of the inventor(s) (35 U.S.C. 371 (c)(4)). (unsigned)
11. ☐ A copy of the International Preliminary Examination Report (PCT/IPEA/409).
12. ☐ A translation of the annexes to the International Preliminary Examination Report under PCT Article 36 (35 U.S.C. 371 (c)(5)).

Items 13 to 20 below concern document(s) or information included:

13. ☒ An Information Disclosure Statement under 37 CFR 1.97 and 1.98. w/Form 1449 and cited prior art.
14. ☐ An assignment document for recording. A separate cover sheet in compliance with 37 CFR 3.28 and 3.31 is included.
15. ☐ A **FIRST** preliminary amendment.
16. ☐ A **SECOND** or **SUBSEQUENT** preliminary amendment.
17. ☐ A substitute specification.
18. ☐ A change of power of attorney and/or address letter.
19. ☒ Certificate of Mailing by Express Mail
20. ☒ Other items or information:

- a.) Forms PCT/IB/301, 304, 308 and 346
- b.) PCT Request Easy;
- c.) Thirty-six (36) sheets of formal drawings;
- d.) Copy of front page of PCT Published Application No. WO/00/49510 as published on August 24, 2000;
- e.) Certified translation of Japanese priority patent application No. P11-039218 filed on February 17, 1999.

The check amount it doesn't match with  
the fee calculation sheet.

U.S. APPLICATION NO. (IF KNOWN, SEE 37 CFR 1.5)		INTERNATIONAL APPLICATION NO.		ATTORNEY'S DOCKET NUMBER	
09/647378		PCT/JP00/00904		KOIK-T0185	
21. The following fees are submitted:				CALCULATIONS PTO USE ONLY	
<b>BASIC NATIONAL FEE (37 CFR 1.492 (a) (1) - (5)) :</b> <input type="checkbox"/> Neither international preliminary examination fee (37 CFR 1.482) nor international search fee (37 CFR 1.445(a)(2)) paid to USPTO and International Search Report not prepared by the EPO or JPO ..... \$970.00 <input checked="" type="checkbox"/> International preliminary examination fee (37 CFR 1.482) not paid to USPTO but International Search Report prepared by the EPO or JPO ..... \$840.00 <input type="checkbox"/> International preliminary examination fee (37 CFR 1.482) not paid to USPTO but international search fee (37 CFR 1.445(a)(2)) paid to USPTO ..... \$690.00 <input type="checkbox"/> International preliminary examination fee paid to USPTO (37 CFR 1.482) but all claims did not satisfy provisions of PCT Article 33(1)-(4) ..... \$670.00 <input type="checkbox"/> International preliminary examination fee paid to USPTO (37 CFR 1.482) and all claims satisfied provisions of PCT Article 33(1)-(4) ..... \$96.00					
<b>ENTER APPROPRIATE BASIC FEE AMOUNT =</b>				\$840.00	
Surcharge of \$130.00 for furnishing the oath or declaration later than months from the earliest claimed priority date (37 CFR 1.492 (e)). <input type="checkbox"/> 20 <input type="checkbox"/> 30				\$0.00	
CLAIMS	NUMBER FILED	NUMBER EXTRA	RATE		
Total claims	35 - 20 =	15	x \$18.00	\$270.00	
Independent claims	25 - 3 =	22	x \$78.00	\$1,716.00	
Multiple Dependent Claims (check if applicable) <input type="checkbox"/>				\$0.00	
<b>TOTAL OF ABOVE CALCULATIONS =</b>				\$2,826.00	
Reduction of 1/2 for filing by small entity, if applicable. Verified Small Entity Statement must also be filed (Note 37 CFR 1.9, 1.27, 1.28) (check if applicable). <input type="checkbox"/>				\$0.00	
<b>SUBTOTAL =</b>				\$2,826.00	
Processing fee of \$130.00 for furnishing the English translation later than months from the earliest claimed priority date (37 CFR 1.492 (f)). <input type="checkbox"/> 20 <input type="checkbox"/> 30				\$0.00	
<b>TOTAL NATIONAL FEE =</b>				\$2,826.00	
Fee for recording the enclosed assignment (37 CFR 1.21(h)). The assignment must be accompanied by an appropriate cover sheet (37 CFR 3.28, 3.31) (check if applicable). <input type="checkbox"/>				\$0.00	
<b>TOTAL FEES ENCLOSED =</b>				\$2,826.00	
				Amount to be refunded	\$
				charged	\$
<input checked="" type="checkbox"/> A check in the amount of <b>\$2,826.00</b> to cover the above fees is enclosed. <input type="checkbox"/> Please charge my Deposit Account No. _____ in the amount of _____ to cover the above fees. A duplicate copy of this sheet is enclosed. <input checked="" type="checkbox"/> The Commissioner is hereby authorized to charge any fees which may be required, or credit any overpayment to Deposit Account No. <b>12-1420</b> A duplicate copy of this sheet is enclosed.					
<b>NOTE: Where an appropriate time limit under 37 CFR 1.494 or 1.495 has not been met, a petition to revive (37 CFR 1.137(a) or (b)) must be filed and granted to restore the application to pending status.</b>					
SEND ALL CORRESPONDENCE TO:					
Charles P. Sammut, Esq. Limbach & Limbach L.L.P. 2001 Ferry Building San Francisco, CA 94111-4262			_____ SIGNATURE  <b>Mayumi Maeda</b> NAME  <b>40,075</b> REGISTRATION NUMBER  <b>September 28, 2000</b> DATE		

36/ppts  
1

09/647378

430 Rec'd PCT/PTO 28 SEP 2000

## DESCRIPTION

### Information Processing Apparatus and Method, and Program Storage Medium

#### Technical Field

The present invention relates to an information processing apparatus and method, and to a program storage medium, and more specifically, to an information processing apparatus and method adapted to prevent falsification of a software used with data in order to inhibit fraudulent copying of the data, and a program storage medium having recorded therein an information processing program for the prevention of the fraudulent copying.

#### Background Art

Recently, as the digital technology has advanced and has become more popular, it has become possible to digitally record or play back a variety of music data, image data, etc. to or from a recording medium. As a result, it has become possible to obtain data not lower in image or sound quality than its original data even after repeating data copying a plurality of times.

With the development of the digital technology, however, the following problems have occurred:

- (1) For example, when a digital music data is copied from a compact disc

(CD) to a hard disc of a personal computer, the music data from the CD can be recorded as it is or compressed into the hard disc, so that the music data will be distributed fraudulently in a large volume via a network such as the Internet.

(2) When a digital music data is copied from a CD to a hard disc of a personal computer, the music data will be distributed in a large volume since the number of copies is not limited.

(3) When a digital music data is copied from a hard disc of a personal computer to an external apparatus such as portable device, the original digital music data will remain in the hard disc after the copying, so that it will possibly be copied and distributed in a large volume.

(4) To prevent the problem (3) above, the software for the personal computer should be designed so that after the digital music data is copied to the external apparatus, the data in the hard disc being the data source is erased (the music data is moved). However, if the content in the hard disc is backed up in another recording medium before it is moved and the data thus backed up is restored to the hard disc after the move, the data having been moved will remain in the hard disc.

(5) When a digital music data in a hard disc of a personal computer is copied to an external apparatus such as portable device, it will possibly be passed to an illegal apparatus since it is not confirmed of what type the external apparatus is.

When a digital music data is passed from an external apparatus such as portable device to a personal computer, it will possibly be passed to an illegal

software since it is not confirmed of what type the software controlling the personal computer is.

(6) When a music data reproduced from a CD is dealt with in a personal computer, ISRC (International Standard Recording Code) included in the music data can be used to judge whether one music piece is the same as the other. However, no ISRC data is included in the CD as the case may be. In this case, it is not possible to judge whether the music pieces are the same as each other.

(7) The above functions can be performed under the control of a software in a personal computer. So, if the software itself is altered, an operation not intended by the system designer will possibly be done.

#### Disclosure of the Invention

Accordingly, the present invention has an object to overcome the above-mentioned drawbacks of the prior art by providing an information processing apparatus and method adapted to positively prevent data from being fraudulently copied in a large volume by analyzing and falsifying a software used with the data, and a program storage medium having recorded therein the information processing program.

An information processing apparatus according to the present invention comprises means for storing content data, a controlling means having a software which controls storage or read of the content data into or from the content data storage means

and means provided in a hardware independent of the controlling means to decrypt and execute an encrypted program supplied from the controlling means and supply the result of the program execution to the controlling means; the controlling means controlling the content data storage or read to or from the content data storage means based on the program execution result supplied from the program executing means. In the information processing apparatus, the content data storage means stores also management information with which the content data stored in itself is managed, and the controlling means makes the program executing means execute a predetermined computation based on the management information. Also, the controlling means may be a CPU, the content data storing means may be a hard disc, and the program executing means may be a CPU incorporated in a semiconductor IC other than a one in which the CPU as the controlling means is built.

Also, the above object can be attained by providing an information processing method including, according to the present invention, a step of controlling storage or read of content data into or from content data storage means based on a result of a program execution by a program executing means.

Also, the above object can be attained by providing a program storage medium having recorded therein a program including, according to the present invention, a step of controlling storage or read of content data into or from a content data storing means based on a result of a program execution by a program executing means.

Also the above object can be attained by providing an information processing

apparatus including, according to the present invention, means for inputting content data, means for storing the content data supplied from the input means, means for compressing the content data stored in the content data storing means in a predetermined manner, means for encrypting the data stored in the content data storing means in a predetermined manner, and means for controlling storage or read, into or from the content data storing means, of the content data compressed by the compressing means and encrypted by the encrypting means.

Also the above object can be attained by providing an information processing method including, according to the present invention, steps of inputting data, storing the data supplied from the data input step, compressing the data stored at the data storing step in a predetermined manner, encrypting the data stored at the data storing step in a predetermined manner, and controlling storage or read of the data compressed at the compressing step and encrypted at the encrypting step.

Also, the above object can be attained by providing a program storage medium having recorded therein a program intended for execution by an information processing apparatus and readable by a computer, the program including, according to the present invention, steps of inputting data, storing the data supplied from the data input step, compressing the data stored at the data storing step in a predetermined manner, encrypting the data stored at the data storing step in a predetermined manner, and controlling storage or read of the data compressed at the compressing step and encrypted at the encrypting step.

Also, the above object can be attained by providing an information processing apparatus including, according to the present invention, means for inputting content data, means for storing the content data supplied from the content data input means, means for holding management information for the content data stored in the content data storing means, means for making a predetermined computation based on the management information held in the management information holding means, and means for controlling the usage of the content data stored in the content data storing means according to a result of a comparison made between the result of the computation made by the computing means and that of a past computation which is stored in the content data storing means.

Also, the above object can be attained by providing an information processing method including, according to the present invention, the steps of inputting data, storing the data supplied from the data input step, holding management information for the data stored at the data storing step, making a predetermined computation based on the management information held at the management information holding step, storing the result of the computation made at the computing step, and controlling the usage of the data stored at the data storing step according to a result of a comparison made between the result of the computation made at the computing step and that of a past computation stored at the data storing step.

Also, the above object can be attained by providing a program storage medium having recorded therein a program intended for execution by an information



processing apparatus and readable by a computer, the program including, according to the present invention, the steps of inputting data, storing the data supplied from the data input step, holding management information for the data stored at the data storing step, making a predetermined computation based on the management information held at the management information holding step, storing the result of the computation made at the computing step, and controlling the usage of the data stored at the data storing step according to a result of a comparison made between the result of the computation made at the computing step and that of a past computation stored at the data storing step.

Also, the above object can be attained by providing an information processing apparatus including, according to the present invention, means for transmitting and receiving data to and from other apparatus, means for holding a predetermined lock key and save key, authenticating means which uses the lock key held in the holding means when transmitting and receiving data to and from the other apparatus to make a mutual authentication with the other apparatus to generate a communication key, means for encrypting the communication key with the save key, and means for storing the data received by the data transmitting and receiving means and having been encrypted with the communication key correspondingly to the communication key encrypted by the encrypting means.

Also, the above object can be attained by providing an information processing method including, according to the present invention, the steps of transmitting and

receiving data to and from other apparatus, holding a predetermined lock key and save key, using the lock key held at the holding step when transmitting and receiving data to and from the other apparatus to make a mutual authentication with the other apparatus to generate a communication key, encrypting the communication key with the save key, and storing the data received at the data transmitting and receiving step and having been encrypted with the communication key correspondingly to the communication key encrypted at the encrypting step.

Also, the above object can be attained by providing a program storage medium having recorded therein a program intended for execution by an information processing apparatus and readable by a computer, the program including, according to the present invention, the steps of transmitting and receiving data to and from other apparatus, holding a predetermined lock key and save key, using the lock key held at the holding step when transmitting and receiving data to and from the other apparatus to make a mutual authentication with the other apparatus to generate a communication key, encrypting the communication key with the save key, and storing the data received at the data transmitting and receiving step and having been encrypted with the communication key correspondingly to the communication key encrypted at the encrypting step.

Also, the above object can be attained by providing an information processing apparatus including according to the present invention means for storing data, means for holding the usage rule for the data stored in the data storing means, means for

judging whether or not, when moving the data stored in the data storing means to other apparatus, the usage rule for the data stored in the data storing means is reproducible by the other apparatus, and means for moving, based on the result of the judgment by the judging means, the data stored in the data storing means to the other apparatus along with the usage rule for the data stored in the data storing means, which is held in the holding means.

Also, the above object can be attained by providing an information processing method including, according to the present invention, the steps of storing data, holding the usage rule for the data stored at the data storing step, judging whether or not, when moving the data stored at the data storing step to other apparatus, the usage rule for the data stored at the data storing is reproducible by the other apparatus, and moving, based on the result of the judgment at the judging step, the data stored in the data storing means to the other apparatus along with the usage rule for the data stored at the data storing step, which is held at the holding step.

Also, the above object can be attained by providing a program storage medium having recorded therein a program intended for execution by an information processing apparatus and readable by a computer, the program including, according to the present invention, the steps of storing data, holding the usage rule for the data stored at the data storing step, judging whether or not, when moving the data stored at the data storing step to other apparatus, the usage rule for the data stored at the data storing step is reproducible by the other apparatus, and moving, based on the result

of the judgment at the judging step, the data stored in the data storing means to the other apparatus along with the usage rule for the data stored at the data storing step, which is held at the holding step.

### Brief Description of the Drawings

FIG. 1 shows an embodiment of a content data management system according to the present invention.

FIG. 2 explains the configuration of a personal computer used in the content data management system.

FIG. 3 explains the configuration of a portable device included in the content data management system.

FIG. 4 is a block diagram of the personal computer for explanation of the functions of the personal computer.

FIG. 5 shows an example of display/operation-instructive window.

FIG. 6 shows an example of the window which the recording program makes the display unit display.

FIG. 7 is a flow chart of operations effected in copying a content from a compact disc to an HDD.

FIG. 8 is a flow chart of operations effected in checking the time limit data base at step S12 in the flow chart shown in FIG. 7.

FIG. 9 shows an example of the time limit data base.

FIG. 10 explains a water mark.

FIG. 11 shows an example of music data base.

FIG. 12 is a flow chart of operations effected in moving a content from the HDD to portable device.

FIG. 13 is a flow chart of operations effected in moving a content from the HDD to portable device.

FIG. 14 is a flow chart of operations effected in moving a content from the HDD to portable device.

FIG. 15 is a flow chart of operations effected in checking conditions for playback of a selected content at step S55 in the flow chart shown in FIG. 12.

FIG. 16 explains the playback conditions managed by the portable device.

FIG. 17 is a flow chart of operations effected in format conversion at step S58 in the flow chart in FIG. 12.

FIG. 18 is a flow chart of operations effected in copying a content from the HDD to portable device.

FIG. 19 is a flow chart of operations effected in copying a content from the HDD to portable device.

FIG. 20 is a flow chart of operations effected in copying a content from the HDD to portable device.

FIG. 21 is a flow chart of operations effected in copying a content from the portable device to HDD.

FIG. 22 is a flow chart of operations effected in copying a content from the portable device to HDD.

FIG. 23 is a flow chart of operations effected in copying a content from an EMD server to HDD.

FIG. 24 is a flow chart of operations effected in accounting at step S204 in the flow chart shown in FIG. 23.

FIG. 25 explains a accounting log.

FIG. 26 is a flow chart of operations effected in copying a content to the HDD from an IEC60958 terminal of the personal computer.

FIG. 27 is a flow chart of operations effected in copying a content to the HDD from an IEC60958 terminal of the personal computer.

FIG. 28 is a flow chart of operations effected in outputting a content from the HDD to the IEC60958 terminal.

FIG. 29 is a flow chart of operations effected in outputting a content from the HDD to the IEC60958 terminal.

FIG. 30 is a flow chart of operations in checking playback conditions at step S275 in the flow chart shown in FIG. 28.

FIG. 31 is a flow chart of operations effected in outputting a content from the HDD via the portable device.

FIG. 32 is a flow chart of operations effected in outputting a content from the HDD via the portable device.

FIG. 33 explains the function of a nonvolatile memory.

FIG. 34 is a flow chart of operations of the adaptor.

FIG. 35 shows the internal construction of the adaptor.

FIGS. 36A and 36B show examples, respectively, of the internal construction of the nonvolatile memory.

FIG. 37 shows an example of the internal construction of the nonvolatile memory.

### Best Mode for Carrying Out the Invention

The best mode for carrying out the present invention will be described in further detail herebelow with reference to the accompanying drawings.

FIG. 1 shows an embodiment of the content data management system according to the present invention. The content data management system includes a personal computer 1 connected to a network 2 composed of a local area network or Internet. The personal computer 1 compresses a music data (will be referred to as "content" hereinafter) received from EMD (Electrical Music Distribution) servers 4-1 to 4-3 or read from a CD (Compact Disc) which will further be described later in a predetermined manner (ATRAC3 (trademark) for example), and encrypts the compressed content, for recording, by an encrypting method such as DES (Data Encryption Standard) or the like.

The personal computer 1 records also, for an encrypted and recorded content,

a usage rule according to which the content is to be used.

The usage rule shows, for example, a number of portable devices (abbreviated as “PD” as the case may be) which can simultaneously use the content following the usage rule. The number of PDs referred to herein is a number of PDs which can check out the content as will further described later. Even after a number of contents included in the usage rule has been checked out, the personal computer 1 can play back the content.

Otherwise, the usage rule may show that the content can be copied. When the content is copied to portable devices 6-1 to 6-3, the personal computer 1 can play back the recorded content. The content can be stored into the portable devices 6-1 to 6-3 a number of times which is limited as the case may be. In this case, the content can be copied a number of times which will not be increased.

Alternatively, the usage rule may show that the content can be moved to other personal computer. After the content is moved to the portable devices 6-1 to 6-3, the content recorded in the personal computer 1 cannot be used (the content is deleted or the usage rule are changed).

The usage rule will be described in detail later.

The personal computer 1 will store the encrypted and recorded content along with the content-related data (e.g., title of, or playback condition for, each music piece) into the connected portable device 6-1 via a USB (Universal Serial Bus) cable 7-1, and update the usage rule for the stored content in response to the content storage into the



portable device 6-1 (which operations will be referred to as “check-out” hereinafter). More specifically, when the content is checked out, the number of times a content can be checked out, included in the usage rule for the content and recorded in the personal computer 1, is decreased by one. Therefore, when the number of times a content can be checked out becomes zero, the content following the usage rule cannot be checked out any longer.

Also, the personal computer 1 will store the encrypted and recorded content along with the content-related data into the connected portable device 6-2 via a USB cable 7-2, and update the usage rule for the stored content in response to the content storage into the portable device 6-2. Further, the personal computer 1 will store the encrypted and recorded content along with the content-related data into the connected portable device 6-3 via a USB (Universal Serial Bus) cable 7-3, and update the usage rule for the stored content in response to the content storage into the portable device 6-3.

Also, the computer 1 will make the portable device 6-1 connected thereto by the USB cable 7-1 delete, or disable the portable device 6-1 to use, the content the personal computer 1 has checked out, thereby updating the usage rule for the deleted content (which operation will be referred to as “check-in” hereinafter). More specifically, when the content has been checked in, the number of times a content can be checked out, included in the usage rule for the content and recorded in the personal computer 1, is increased by one.

Also, the computer 1 will make the portable device 6-2 connected thereto by the USB cable 7-2 delete, or disable the portable device 6-2 to use, the content the personal computer 1 has checked out, thereby updating the usage rule for the deleted content. Further, the computer 1 will make the portable device 6-3 connected thereto by the USB cable 7-3 delete, or disable the portable device 6-3 to use, the content the personal computer 1 has checked out, thereby updating the usage rule for the deleted content.

The personal computer 1 cannot check in a content which other personal computer (not shown) has checked out to the portable device 6-1. Also, The personal computer 1 cannot check in a content which the other personal computer has checked out to the portable device 6-2. Further, the personal computer 1 cannot check in a content which the other personal computer has checked out to the portable device 6-3.

As shown, the content data management system according to the present invention includes also an EMD registration server 3. When the personal computer 1 starts acquiring the content from the EMD servers 4-1 to 4-3, the EMD registration server 3 responds to a request from the personal computer 1 to transmit to the personal computer 1 via the network 2 an authenticate key necessary for mutual authentication between the personal computer 1 and EMD servers 4-1 to 4-3, and to the personal computer 1 a program for connection to the EMD servers 4-1 to 4-3.

In response to the request from the personal computer 1, the EMD server 4-1 will supply a content along with a content-related data (e.g., title or playback limit of

each music piece) to the personal computer 1 via the network 2. Also, the EMD server 4-2 will respond to the request from the personal computer 1 to supply a content along with a content-related data to the personal computer 1 via the network 2. Further, in response to the request from the personal computer 1, the EMD server 4-3 will supply a content along with a content-related data to the personal computer 1 via the network 2.

The contents supplied from the EMD servers 4-1 to 4-3 are compressed in the same manner or in different manners, respectively. Also, the contents supplied from the EMD servers 4-1 to 4-3 are encrypted in the same manner or different manners, respectively.

As shown, the content data management system according to the present invention includes also WWW (world-wide web) servers 5-1 and 5-2. The WWW server 5-1 responds to the request from the personal computer 1 to supply the personal computer 1 via the network 2 with a CD from which a content has been read (e.g., CD album name or CD supplier) and data corresponding to the read content (e.g., title or composer's name of each music piece). In response to the request from the personal computer 1, the WWW server 5-2 supplies the personal computer 1 via the network 2 with a CD from which a content has been read and data corresponding to the read content.

The portable device 6-1 stores the content supplied from the personal computer 1 (i.e., a checked-out content) along with data related with the content (e.g., title or

playback limit of each music piece). Based on the content-related data, the portable device 6-1 will play back and output the stored content to a headphone or the like (not shown).

For example, when it is tried to play back a content a larger number of times than a playback limit stored as the content-related data, the portable device 6-1 will stop playback of the corresponding content. Also, when it is tried to play back after a playback time limit stored as the content-related data has passed, the portable device 6-1 will stop playback of the corresponding content.

The user will be able to disconnect, for carrying, the portable device 6-1 having a content stored therein from the personal computer 1, and play back the content stored in the portable device 6-1 for listening to a music piece corresponding to the content through the headphone or the like.

The portable device 6-2 stores the content supplied from the personal computer 1 along with data related with the content. Based on the content-related data, the portable device 6-2 will play back and output the stored content to a headphone or the like (not shown). The user will be able to disconnect, for carrying, the portable device 6-2 having a content stored therein from the personal computer 1, and play back the content stored in the portable device 6-2 for listening to a music piece corresponding to the content through the headphone or the like.

The portable device 6-3 stores the content supplied from the personal computer 1 along with data related with the content. Based on the content-related data, the

portable device 6-3 will play back and output the stored content to a headphone or the like (not shown). The user will be able to disconnect, for carrying, the portable device 6-3 having a content stored therein from the personal computer 1, and play back the content stored in the portable device 6-3 for listening to a music piece corresponding to the content through the headphone or the like.

The portable devices 6-1 to 6-3 will be referred to simply as “portable device 6” hereafter wherever they may not be referred to individually.

FIG. 2 is an explanatory illustration of the configuration of the personal computer 1. As shown, the personal computer 1 comprises a CPU (central processing unit) 11. The CPU 11 actually executes a variety of applications (will further be described later) and OS (operating system). A ROM (read-only memory) 12 is also provided in the personal computer 1, and generally stores basically fixed data of programs and computational parameters used in the CPU 11. Also, a RAM (random-access memory) 13 is included in the personal computer 1 to store programs used for execution of the applications and OS by the CPU 11 and parameters which are appropriately variable in the execution of the applications and OS. The CPU 11, ROM 12 and RAM 13 are mutually connected to each other by a host bus 14 composed of a CPU bus, etc.

The host bus 14 is connected to an external bus 16 such as PCI (peripheral component interconnect/interface) by a bridge 15.

The personal computer 1 is also provided with a keyboard 18 which is operated

by the user to input various commands to the CPU 11, and with a mouse 19 which is used by the user to point and select a point on the screen of a display unit 20. The display unit 20 is a liquid crystal display or CRT (cathode-ray tube) to display a variety of information in the form of a text and/or image. Further, the personal computer 1 is provided with an HDD (hard disc drive) 21 which drives a hard disc to write or read a program to be executed by the CPU 11 and information to or from the hard disc.

A drive 22 is also provided in the personal computer 1. The drive 22 reads data or program recorded in any of a magnetic disc 41, optical disc 42 (including CD), magneto-optical disc 43 and semiconductor memory 44, whichever is connected to the drive 22, and supplies the read data or program to the RAM 13 connected thereto by an interface 17, external bus 16, bridge 15 and host bus 14.

The personal computer 1 is also provided with USB ports 23-1, 23-2 and 23-3. The USB port 23-1 has the portable device 6-1 connected thereto by the USB cable 7-1, and outputs data (including a content or a command to the portable device 6-1, for example) supplied from the HDD 21, CPU 11 or RAM 13 to the portable device 6-1 via the interface 17, external bus 16, bridge 15 or host bus 14.

The USB port 23-2 has the portable device 6-2 connected thereto by the USB cable 7-2, and outputs data (including a content or a command to the portable device 6-2, for example) supplied from the HDD 21, CPU 11 or RAM 13 to the portable device 6-2 via the interface 17, external bus 16, bridge 15 or host bus 14.

The USB port 23-3 has the portable device 6-3 connected thereto by the USB

cable 7-3, and outputs data (including a content or a command to the portable device 6-3, for example) supplied from the HDD 21, CPU 11 or RAM 13 to the portable device 6-3 via the interface 17, external bus 16, bridge 15 or host bus 14.

The personal computer 1 is also provided with an audio input/output interface 24 having an IEC (International Electrotechnical Commission) 60958 terminal 24a. The audio input/output interface 24 interfaces a digital audio input/output or an analog audio input/output. The personal computer 1 has also a speaker 45 which provides a predetermined sound corresponding to each content based on an audio signal supplied from the audio input/output interface 24.

The accessories including the keyboard 18 to audio input/output interface 24 are connected to the interface 17 which in turn is connected to the CPU 11 by the external bus 16, bridge 15 and host bus 14.

Further, the personal computer 1 has a communications block 25 connected to the network 2. The communications block 25 transmits, as stored in packets in a predetermined manner, data (e.g., request for registration or request for sending a content) supplied from the CPU 11 or HDD 21 via the network 2 while outputting data (e.g., authenticate key or content) stored in received packets to the CPU 11, RAM 13 or HDD 21 via the network 2.

An adaptor 26 formed integrally as a semiconductor IC is also provided for connection to the personal computer 1. It has a CPU 32, RAM 33, nonvolatile memory 34, RTC (real-time clock) 35 and a ROM 36. The CPU 32 is connected to

the CPU 11 in the personal computer 1 by the external bus 16, bridge 15 and host bus 14 and thus cooperates with the CPU 11 to effect various processes. The RAM 33 stores data and programs necessary for execution of the various processes by the CPU 32. The nonvolatile memory 34 stores data which have to be held still after the personal computer 1 is turned off. The ROM 36 stores a program for decryption of an encrypted program transferred from the personal computer 1. The RTC 35 keeps time to provide time information.

The communications block 25 and adaptor 26 are connected to the CPU 11 by the external bus 16, bridge 15 and host bus 14.

The USB ports 23-1 to 23-3 will be referred to simply as “USB port 23” hereafter wherever they have not to be referred to individually. Also, the USB cables 7-1 to 7-3 will be referred to simply as “USB cable 7” hereafter wherever they have not to be referred to individually.

Referring now to FIG. 3, the portable device 6 is schematically illustrated in the form of a block diagram. The portable device 6 includes a power circuit 52 which converts a voltage supplied from a dry cell 51 to an internal power of a predetermined voltage. Supplying the power to components from a CPU 53 to display unit 67, the power circuit 52 will thus drive the entire portable device 6.

A USB controller 57 is provided in the portable device 6. When connected to the personal computer 1 by a USB connector 56 and USB cable 7, the USB controller 57 will supply data including a content transferred from the personal computer 1 to the



CPU 53 via an internal bus 58.

A data to be transferred from the personal computer 1 is composed of data of 64 bytes per packet, and transferred from the personal computer 1 at a transfer rate of 12 Mbits/sec.

A data to be transferred to the portable device 6 is composed of a header and content. The header stores a content ID, file name, header size, content key, file size, codec ID, file information, etc. and also a playback limitation data, start date, end date, playback limit, playback counter, etc., necessary for the playback limitation. It should be noted here that the term “date” used herein refers to a date and time. The content is coded by the encoding method such as ATRAC3 and encrypted.

The header size indicates a data length of a header (e.g., 33 bytes), and the file size indicates a data length of the content (e.g., 33,636,138 bytes).

The content key is a key for decryption of an encrypted content, and transmitted from the personal computer 1 to the portable device 6 in a format encrypted based on a session key (provisional) generated via a mutual authentication between the personal computer 1 and portable device 6.

When the portable device 6 is connected to the USB port 23 of the personal computer 1 by the USB cable 7, there will be made a mutual authentication between the portable device 6 and personal computer 1. This mutual authentication is of a challenge-response type for example. Note that a DSP (digital signal processor) 59 is also provided in the portable device 6 to decrypt an encrypted content when the

challenge-response type authentication is done.

The above-mentioned challenge-response type mutual authentication is such that in response to a certain value (challenge) generated by the personal computer, for example, there is generated a value (response) by the portable device 6 by using a private key common to both the portable device 6 and personal computer 1. In the challenge-response type mutual authentication, the value generated by the personal computer 1 varies at every authentication. So, even when for example a value generated using the private key and outputted from the portable device 6 is read, that is, a so-called disguised attack takes place, the personal computer 1 can detect a fraudulence since a next mutual authentication is done using a different value.

The content ID is an ID for a content to identify the content.

The codec ID is an ID corresponding to an encoding method for a content. For example, a codec ID of "1" corresponds to ATRAC3 while a codec ID of "0" corresponds to MP3 (MPEG (Moving Picture Experts Group) Audio Layer-3).

The file name is a data resulted from conversion of a content file (will further be described later) corresponding to a content and recorded in the personal computer 1 to an ASCII (American National Standard Code for Information Interchange) code. The file information is a data resulted from conversion of a music piece title (content name), name of the artist playing the music piece, name of the songwriter of the music piece or name of the composer of the music piece to an ASCII code.

The playback limitation data is to indicate whether there is set a playback period

for which a content can be played back (i.e., start date or end date) or a playback limit (a limited number of times) a content can be played back. When a playback limit is set, the playback limitation data is assigned “1”. When a period for which a content can be played back is set, the playback limitation data is assigned “2”. When there is neither a playback limit nor a playback period (namely, when the content is purchased), the playback limitation data is assigned “0”.

The start date and end date are data indicating a range of a period for which a content can be played back when the playback limitation data is assigned “2”. For example, when the start date is “00040F” while the end date is “00070F”, a corresponding content can be played back for a period from April 15, 2000 until July 15, 2000.

Similarly, the playback limit and playback counter are as follows. Namely, when the playback limitation data is assigned “1” or “2”, the playback limit is a predetermined number of times a content can be played back, and the playback counter is a number of times the content has been played back and which is updated by the CPU 53 upon completion of that playback. For example, when the playback limit is “02”, the content can be played back two times. When the playback counter is “01”, it means that the content has been played back once.

When the playback limitation data is assigned “2”, the start date is “00040F”, end date is “00070F” and the playback limit is “02”, for example, the portable device 6 will be permitted to play back a corresponding content twice a day for a period from

April 15, 2000 until July 15, 2000.

Also, when the playback limitation data is assigned "1", start date is "000000", end date is "000000", playback limit is "0" and playback counter is "05", for example, a corresponding content can be played back for an unlimited period, can be played back 10 times, and has been played back 5 times.

When the portable device 6 receives a content and a content write command from the personal computer 1, the CPU 53 which executes a main program read from a ROM 55 to RAM 54, will receive the write command, control a flash memory controller 60 and write to a flash memory 61 the content received from the personal computer 1.

The flash memory 61 has a storage capacity of about 64 Mbytes to store the content. Also, the flash memory has stored therein in advance a playback code for expansion of a content having been compressed in a predetermined manner.

Note that the flash memory 61 may be formed as a memory card which is connectable to, and removable from, the portable device 6.

When the CPU 53 is supplied with a playback command corresponding to a push-down operation of a play/stop button (not shown) via an operation key controller 62, it will make the flash memory controller 60 read the playback code and content from the flash memory 61 and transfer them to the DSP 59 of the portable device 6.

After detecting error in the content in the CRC (cyclic redundancy check) method according to the playback code transferred from the flash memory 61, the DSP

59 will play back the content and the played-back data (indicated with a reference D1 in FIG. 3) to a digital/analog conversion circuit 63.

The DSP 59 is formed integrally with a transmission circuit (not shown) provided inside the portable device 6 to play back a content based on a master clock MCLK from an external crystal oscillator 59A, and supplies the digital/analog conversion circuit 63 with the master clock MCLK, a bit clock BCLK generated by an internal oscillation circuit based on the master clock MCLK and having a predetermined frequency, and an operating clock LRCLK composed of an L-channel clock LCLK and R-channel clock RCLK in the units of frames.

For playing back a content, the DSP 59 will supply the above-mentioned operating clock to the digital/analog conversion circuit 63 according to the playback code. When playing back no content, the DSP 59 will stop supplying the operating clock according to the playback code to turn off the digital/analog conversion circuit 63, thereby reducing the power consumption of the entire portable device 6.

Similarly, the CPU 53 and USB controller 57 have external crystal oscillators 53A and 57A connected thereto, respectively, and effect predetermined operations on the basis of master clocks MCLK supplied from the oscillators 53A and 57A, respectively.

Because of the above-mentioned construction, the portable device 6 needs no clock generation module to supply a clock to each of the CPU 53, DSP 59 and USB controller 57 and thus can be designed to have a simpler and more compact circuit

construction.

The digital/analog conversion circuit 63 converts a played-back content to an analog audio signal and supplies it to an amplification circuit 64. The amplification circuit 64 amplifies the audio signal and supplies it to headphone (not shown) via a headphone jack 65.

Thus, when the play/stop button (not shown) is pressed, the portable device 6 plays back a content stored in the flash memory 61 under the control of the CPU 53. When the play/stop button is pressed in the course of playing back a content, the portable device 6 will stop playing back the content.

When the play/stop button is pressed after stopping the content playback operation, the portable device 6 will resume the content playback at the position where the playback operation has been stopped under the control of the CPU 53. When a time of a few seconds has passed with no additional operation effected after the playback operation is stopped by pressing the play/stop button, the portable device 6 will automatically shut off the power supply, thereby reducing the power consumption.

It should be noted here that when the play/stop button is pressed after the power supply is turned off, the portable device 6 will resume the playback at the first music piece or music piece No. 1 without playing back the content at the position where the playback operation has previously been stopped.

Also, the CPU 53 of the portable device 6 makes an LCD controller 68 display on a display unit 67 a playback mode (e.g., repeated play, introducing play, etc),

equalization adjustment (i.e., gain adjustment for a frequency band of the audio signal), number for music piece, playing time, operation modes such as play, stop, fast forward and fast rewind, and information such as sound volume and voltage level in the dry cell 51.

Further, the portable device 6 stores into an EEPROM 68 a number of contents written in a flash memory 80, locations of blocks of the flash memory 61 in which contents are written, respectively, and a so-called FAT (file allocation table) for various information stored in the memory.

It should be noted that in this embodiment, a content is taken as one block of 64 kbytes and a location of the block for the content of each music piece is stored in the FAT.

In case a FAT is stored into the flash memory 61, when the content of a first music piece is written into the flash memory 61 under the control of the CPU 53, the location of a block corresponding to the content of the first music piece will be written as FAT into the flash memory, and then when the content of a second music piece is written into the flash memory 61, the location of a block corresponding to the content of the second music piece will be written as FAT into the flash memory 61 (in the same area as that in which the first music piece has already been written).

In this way, a FAT is rewritten each time the content is written into the flash memory 61 and further the same data will be written again for reservation to protect the data.

When FAT is written into the flash memory 61, the same area in the flash memory will be rewritten twice correspondingly to the write of the first content. For this reason, when content write has been made a small number of times, a specified number of times for rewrite of the flash memory 61 will be reached, so that the flash memory 61 will not be rewritable any longer.

To avoid the above, the portable device 6 makes the EEPROM 68 store FAT so that FAT will be rewritten a reduced number of times in the flash memory 61 at write of each content.

By storing into the EEPROM 68 a FAT which is rewritten a large number of times, the portable device 6 can be adapted such that content can be written into the flash memory 61 at a frequency tens times larger than that at which FAT is stored into the flash memory 61. Further, since the CPU 53 makes the EEPROM 68 additionally store FAT, the same area in the EEPROM 68 is rewritten at a reduced frequency to prevent the EEPROM 68 from early becoming not rewritable.

When the portable device 6 is connected to the personal computer 1 by the USB cable 7 (which will be referred to as “USB connection” hereinafter), it is recognized based on an interrupt signal supplied from the USB controller 57 to the CPU 53 that the USB connection has been made.

When the portable device 6 recognizes the USB connection, it is supplied with an external power of a specified current value from the personal computer 1 via the USB cable 7, and makes a power circuit 52 stop the power supply from the dry cell 51.



When the USB connection is established, the CPU 53 will stop the DSP 59 from playing back a content. Thus, the CPU 53 will prevent the external power supplied from the personal computer 1 from exceeding the specified current value so that the external power of the specified current value can always be supplied.

Thus, when the USB connection is established, the CPU 53 makes a selection between the power supplied from the dry cell 51 and the power supplied from the personal computer 1. That is, the inexpensive external power from the personal computer 1 can be used, and so the costly power supplied from the dry cell 51 and which costs high is less consumed. Thus, the dry cell 51 can be used for a longer service life.

Note that when supplied with the external power from the personal computer 1 via the USB cable 7, the CPU 53 stops the DSP 59 from playing back a content to reduce the radiation from the DSP 59, so that the radiation of the entire system including the personal computer 1 can further be reduced.

Referring now to FIG. 4, there is illustrated a block diagram of the personal computer 1, explaining the functions of the personal computer 1, implemented by execution of predetermined programs by the CPU 11. As shown, the personal computer 1 uses a content management program 111 which is composed of a plurality of programs including an EMD selection program 131, check-in/check-out management program 132, copy management program 133, move management program 134, encryption method conversion program 135, compression method

conversion program 136, encryption program 137, compression/expansion program 138, usage rule conversion program 139, usage rule management program 140, authentication program 141, decryption program 142, PD driver 143, purchase programs 144 and 145.

Of the above programs, the content management program 111 is composed of shuffled or encrypted instructions, for example, to conceal the instructed operations from outside to make it difficult to interpret the instructions (for example, even if the user can read directly the content management program 111, he or she cannot identify the instructions).

The EMD selection program 131 is not included in the content management program 111 when the latter is installed in the personal computer 1 but it is received from the EMD registration server 3 via the network 2 at the time of EMD registration which will further be described later. The EMD selection program 131 selects a connection with any of the EMD servers 4-1 to 4-3 to enable a purchase application program 115, purchase program 144 or 142 to have a communication with any of the EMD servers 4-1 to 4-3 (e.g., download of a content for purchase).

Based on a setting of either check-in or check-out and usage rule files 162-1 to 162-N recorded in a content data base 114, the check-in/check-out management program 132 checks out contents stored in content files 161-1 to 161-N to any of the portable devices 6-1 to 6-3, or checks in contents stored in the portable devices 6-1 to 6-3.

In response to the check-in or check-out having been done, the check-in/check-out management program 132 updates the usage rule stored in the usage rule files 162-1 to 162-N recorded in the content data base 114.

Based on the usage rule files 162-1 to 162-N recorded in the content data base 114, the copy management program 133 copies contents stored in the content files 161-1 to 161-N to any of the portable devices 6-1 to 6-3, or copies contents from the portable devices 6-1 to 6-3 to the content data base 114.

Also based on the usage rule files 162-1 to 162-N recorded in the content data base 114, the move management program 134 moves contents stored in the content files 161-1 to 161-N to any of the portable devices 6-1 to 6-3, or contents from the portable devices 6-1 to 6-3 to the content data base 114.

The encryption method conversion program 135 converts, to the same encryption method as that used with the contents stored in the content files 161-1 to 161-N recorded in the content data base 114, the encryption method used with a content the purchase application program 115 receives from the EMD server 4-1 via the network 2, a content the purchase program 144 receives from the EMD server 4-2 via the network 3 or a content the purchase program 145 receives from the EMD server 4-3 via the network 2.

In addition, to check out a content to the portable device 6-1 or 6-3, the encryption method conversion program 135 converts the encryption method used with the content to be checked out to a one used in the portable device 6-1 or 6-3.

The compression method conversion program 136 converts, to the same compression method as that used with the contents stored in the content files 161-1 to 161-N recorded in the content data base 114, the compression method used with a content the purchase application program 115 receives from the EMD server 4-1 via the network 2, a content the purchase program 144 receives from the EMD server 4-2 via the network 2 or a content the purchase program 145 receives from the EMD server 4-3 via the network 2.

Also, to check out a content to the portable device 6-1 or 6-3, the compression method conversion program 136 converts the compression method used with the content to be checked out to a one used in the portable device 6-1 or 6-3.

The encryption program 137 is used to encrypt a content (not encrypted) read from a CD and supplied from a recording program 113 for example to the same encryption method as that used with contents stored in the content files 161-1 to 161-N recorded in the content data base 114.

The compression/expansion program 138 encodes a content (not compressed) read from a CD and supplied from the recording program 113 by the same encoding method as that used with contents stored in the content files 161-1 to 161-N recorded in the content data base 114. In addition, the compression/expansion program 138 will expand (decrypt) a coded content.

The usage rule conversion program 139 converts, to the same format as that of the usage rule stored in the usage rule files 162-1 to 162-N recorded in the content data

base 114, a usage rule for a content the purchase application program 115 receives from the EMD server 4-1 via the network 2, a content the purchase program 144 receives from the EMD sever 4-2 via the network 2, or a content the purchase program 145 receives from the EMD server 4-3 via the network.

Also, to check out a content to the portable device 6-1 or 6-3, the usage rule conversion program 139 converts the usage rule for the content to be checked out to a one used in the portable device 6-1 or 6-3.

Before execution of content copy, move, check-in or check-out, the usage rule management program 140 detects a falsification or alteration of the usage rules based on hash values (which will further be described later) meeting the usage rules stored in the usage rule files 162-1 to 162-N recorded in the content data base 114. As the usage rules stored in the usage rule files 162-1 to 162-N recorded in the content data base 114 are updated along with a content copy, move, check-in or check-out, the usage rule management program 140 updates the hash values meeting the usage rules.

The authentication program 141 executes a mutual authentication between the content management program 111 and purchase application program 111, and a mutual authentication between the content management program 115 and purchase program 144. Also, the authentication program 141 will store an authenticate key used in the mutual authentication between the EMD server 4-1 and purchase application program 115, a one used in the mutual authentication between the EMD server 4-2 and purchase program 144, and a one used in the mutual authentication between the EMD

server 4-3 and purchase program 145.

It should be noted that when the content management program 111 is installed in the personal computer 1, the authenticate key the authentication program 141 used in the mutual authentication is not yet stored in the authentication program 141 but when a display/operation-instructive program 112 has successfully registered the authenticate key, the key will be supplied from the EMD registration server 3 and stored in the authentication program 141.

The decryption program 142 decrypts a content when the personal computer 1 plays back the content stored in the content files 161-1 to 161-N recorded in the content data base 114.

When checking put a predetermine content to the portable device 6-2 or checking in a predetermined content from the portable device 6-2, the PD driver 143 supplies the portable device 6-2 with the content or a command making the portable device 6-2 do a predetermined operation.

When checking put a predetermine content to the portable device 6-1 or checking in a predetermined content from the portable device 6-1, the PD driver 143 supplies the device driver 116-1 with the content or a command making the device driver 116-1 do a predetermined operation.

When checking put a predetermine content to the portable device 6-3 or checking in a predetermined content from the portable device 6-3, the PD driver 143 supplies the device driver 116-2 with the content or a command making the device

driver 116-2 do a predetermined operation.

The purchase program 144 is a so-called plug-in program. It is installed along with the content management program 111 into the personal computer 1, supplied from the EMD registration server 3 via the network 2, or supplied as recorded in a predetermined CD. When installed in the personal computer 1, the purchase program 144 will transmit or receive the content management program 111 and data via an interface of a predetermined form the content management program 111 has.

The purchase program 144 is composed of shuffled or encrypted instructions, for example, to conceal the instructed operations from outside to make it difficult to interpret the instructions (for example, even if the user can read directly the purchase program 144, he cannot identify the instructions).

The purchase program 144 requests, via the network 2, the EMD server 4-2 to send a predetermined content and thus receives the content from the EMD server 4-2. Upon reception of the content from the EMD server 4-2, the purchase program 144 will account for the content.

The purchase program 145 is to be installed along with the content management program 111. It requests, via the network 2, the EMD server 4-3 to send a predetermined content and thus receives the content from the EMD server 4-3. Upon reception of the content from the EMD server 4-3, the purchase program 145 will account for the content.

Based on a filtering data file 181, display data file 182, image files 183-1 to

183-K or a history data file 184, the display/operation-instructive program 112 displays an image of a predetermined window on the display unit 20, and gives a check-in or check-out instruction to the content management program 111 in response to an operation of the keyboard 18 or mouse 19 by the user.

The filtering data file 181 stores data for weighting contents stored in the content files 161-1 to 161-N recorded in the content data base 114, and is recorded in the HDD 21.

The display data file 182 stores data corresponding to the contents stored in the content files 161-1 to 161-N recorded in the content data base 114, and is recorded in the HDD 21.

The image files 183-1 to 183-N store images corresponding to the content files 161-1 to 161-N recorded in the content data base 114 or images corresponding to packages which will further be described later, and are recorded in the HDD 21.

The image files 183-1 to 183-K will be referred to simply as “image file 183” hereafter wherever they have not be referred to individually.

The history data file 184 stores history data including a number of times the contents stored in the content files 161-1 to 161-N recorded in the content data base 114 have been checked out, a number of times the contents have been checked in, and the dates on which the check-out an check-in were made. The history data file 184 is recorded in the HDD 21.

For the registration, the display/operation-instructive program 112 transmits, via



the network, an ID of the pre-stored content management program 111 to the EMD registration server 3, while receiving, via the network 2, the authenticate key and EMD selection program 131 from the EMD registration server 3 and supplying them to the content management program 111.

The recording program 113 is used to display an image of a predetermined window, and read data such as a recording time of a content from a CD being the optical disc 42 set in the drive 22 in this embodiment in response to an operation of the keyboard 18 or mouse 19 by the user.

Based on a recording time of a content recorded in a CD, the recording program 113 requests, via the network 2, the WWW server 5-1 or 5-2 to send data corresponding to the CD such as album name or artist's name or data corresponding to a content recorded in the CD such as a music piece title, and thus receives, via the network 2, the data corresponding to the CD or the content recorded in the CD from the WWW server 5-1 or 5-2.

Also, the recording program 113 supplies the display/operation-instructive program 112 with the received data corresponding to the CD or data corresponding to the content recorded in the CD.

Further, when supplied with a recording instruction, the recording program 113 reads and outputs to the content management program 111 a content from a CD being the optical disc 42 set in the drive 22 in this embodiment.

The content data base 114 stores into any of the content files 161-1 to 161-N

a content supplied from the content management program 111 and having been compressed in a predetermined manner and encrypted in a predetermined manner (records the content into the HDD 21). The content data base 114 stores usage rules for contents stored in the content files 161-1 to 161-N into any of the usage rule files 162-1 to 162-N corresponding to the content files 161-1 to 161-N in which the contents are stored (records the usage rules into the HDD 21).

The content data base 114 may record the content files 161-1 to 161-N or usage rule files 162-1 to 162-N as records.

A usage rule for a content stored in the content file 161-1 for example is stored in the usage rule file 162-1. A usage rule for a content stored in the content file 161-N is stored in the usage rule file 162-N.

Note that data recorded in the usage rule files 162-1 to 162-N correspond to those recorded in a time limit data base or music data base which will further be described later. Namely, the content data base 114 includes the time limit data base and music data base.

The content files 161-1 to 161-N will be referred to simply as “content file 161” hereinafter wherever they have not be referred to individually. Also, the usage rule files 162-1 to 162-N will be referred to simply as “usage rule file 162” hereafter wherever they have not to be referred to individually.

The purchase application program 115 is supplied from the EMD registration server 3 via the network 2 or as recorded in a predetermined CD-ROM. The purchase

application program 115 requests, via the network 2, the EMD server 4-1 to send a predetermined content, while thus receiving the content from the EMD server 4-1 and supplying it to the content management program 111. Also, upon reception of the content from the EMD server 4-1, the purchase application program 115 will account for the content.

Next, the correspondence between data stored in the display data file 82 and the content files 161-1 to 161-N stored in the content data base 114 will be described herebelow:

Firstly, a content stored in any of the content files 161-1 to 161-N belongs to a predetermined package. More specifically, the package is any of an original package, my selected package and filtering package.

Of the above packages, the original package has more than one content belonging thereto. This package corresponds to the content classification (namely, so-called album) in the EMD servers 4-1 to 4-3 or to one CD. A content belongs to any original package and cannot belong to a plurality of original packages. Also, an original package to which a content belongs cannot be modified. The user can edit a part of information corresponding to an original package (for example, addition of information or change of added information).

More than one content freely selected by the user belong to the my selected package. The user can arbitrarily edit contents for assignment to my selected packages, respectively. A content can belong to more than one my selected package

at a time. Also, a content may not belong to any my selected package.

Contents selected based on a filtering data stored in a filtering data file 181 belong to the filtering package. The filtering data is supplied from the EMD server 4-1 to 4-3 or WWW server 5-1 or 5-2 via the network 2 or as recorded in a predetermined CD. The user can edit the filtering data stored in the filtering data file 181.

The filtering data is a reference for selection of a predetermined content or for calculation of a weight corresponding to the content. For example, filtering data corresponding to top tens of the weekly J-POP (Japan pops) can be used by the personal computer 1 to identify contents of the weekly Japan Pops Nos. 1 to 10.

The filtering data file 181 includes a filtering data for selection of contents in the descending order of the lengths of period for which they have been checked out for the past one month, a filtering data for selection of contents in the descending order of the numbers of times they have been checked out for the past half year, or a filtering data for selection of contents in which a character "AI (love)" is included in the music piece titles (content name).

Thus, contents in the filtering package are selected by comparing a filtering data with a content display data 221 (including data the user has set), a history data 184 or the like.

The driver 117 drives the audio input/output interface 24 under the control of the content management program 111 or the like to input a content being a digital data supplied from outside and supply it to the content management program 111, output

as a digital data a content supplied from the content data base 114 via the content management program 111, or output an analog signal corresponding to a content supplied from the content data base 114 via the content management program 111.

FIG. 5 shows an example of the display/operation-instructive window the display/operation-instructive program 112 makes the display unit 20 display.

There are displayed in the display/operation-instructive window a button 201 for starting up the recording program 113, a button 202 for starting up the EMD selection program 131, a button 203 for displaying a field in which check-in or check-out is set, a button 204 for displaying a field in which a my selected package is to be edited, etc.

When a button 205 is selected, data corresponding to an original package is displayed in a field 211 of the window. When a button 206 is selected, data corresponding to a my selected package is displayed in the field 211. When a button 207 is selected, data corresponding to a filtering package is displayed in the field 211.

Data displayed in the field 211 concerns a package. For example, it is a package name or an artist's name.

As shown in FIG. 5, there are displayed in the field 211 a package name "FIRST" and artist's name "A TARO", a package name "SECOND" and artist's name "A TARO", etc.

The display/operation-instructive window has also a field 212 in which there is displayed data corresponding to a content belonging to a packet selected in the field

211. Data displayed in the field is a music piece title, playing time or a number of times the content can be checked out.

In FIG. 5, a package corresponding to the package name "SECOND" is selected. So, there are displayed in the field 212 the music piece title (content name) "MINAMI-NO-SAKABA" corresponding to the content belonging to the package corresponding to the package name "SECOND", a number of times the content can be checked out (for example, one eighth note is for one check-out and two eighth notes are for two check-out's), and music piece title (content name) "KITA-NO-HAKABA" and number of times the content can be checked (for example, one eighth note corresponds to one check-out).

Thus, one eighth note as a number of times a content can be checked out, displayed in the field 212, indicates that a corresponding content can be checked out once.

A rest as a number of times a content can be checked out, displayed in the field 212, indicates that a corresponding content cannot be checked out (the number of check-out's is zero; however, the personal computer 1 can play back that content). A C clef as a number of times a content can be checked out, displayed in the field 212, indicates that the number of check-out's for a corresponding content is limitless (the content can be checked out any number of times).

Note that the number of times a content can be checked out may be indicated with a corresponding number of pieces of a predetermined figure (for example, it may

be a circle, star, crescent or the like) as shown in FIG. 5 as well as a number.

Also there is displayed in the display/operation-instructive window a field 208 in which an image or the like corresponding to a selected package or content (corresponding to any of the image files 183-1 to 183-K in FIG. 4) is displayed. In this field, a button 209 is clicked when playing back a selected content (outputting a sound corresponding to the content to the speaker 45).

When a music piece title of a predetermined content (content name) displayed in the field 212 is selected and a deleting operation is made while the button 205 is selected and data corresponding to an original package is being displayed in the field 211, the display/operation-instructive program 112 will make the content management program 111 delete the predetermined content stored in the content data base 114, corresponding to the selected music piece title.

When a content read from a CD is recorded into the content data base 114 while a button 255 (which will further be described later) in the window displayed under the control of the recording program 113 is being selected (made active), the display/operation-instructive program 112 will make the display/operation-instructive window display a field 213 in which there is displayed a music piece title of a content (content name) stored in any pre-designated one of the portable devices 6-1 to 6-3.

When a content read from a CD is recorded into the content data base 114 while a button 255 (which will further be described later) in the window displayed under the control of the recording program 113 is being selected (made active), the

display/operation-instructive program 112 will make the content management program 111 check out the content recorded in the content data base 114 and read from the CD to any pre-designated one of the portable devices 6-1 to 6-3.

There is displayed in the field 213 at the leftmost position thereof corresponding to the music piece title of a content (content name) a symbol indicating whether the content can be checked in to the personal computer 1. For example, a symbol “○” at the leftmost position of the field 213 indicates that a content corresponding to a music piece title of a content can be checked in to the personal computer 1 (that is, it has been checked out from the personal computer 1). A symbol “×” at the leftmost position of the field 213 indicates that a content corresponding to a music piece title of a content cannot be checked in to the personal computer 1 (that is, it has not been checked out from the personal computer 1; for example, it has been checked out from any other personal computer).

When the display/operation-instructive program 112 has displayed the field 213 in the display/operation-instructive window, the display/operation-instructive program 112 will display in the display/operation-instructive window a field 214 in which the name of a portable package (to which a content stored in any pre-designated one of the portable devices 6-1 to 6-3 belongs) is displayed, a button 210 to close the field 213, and a button 215 to execute a check-in or check-out operation.

Further, when the display/operation-instructive program 112 has displayed the field 213 in the display/operation-instructive window, the display/operation-instructive



program 112 will display in the display/operation-instructive window a button 216 to set a check-out operation for a content corresponding to a music piece title selected in the field 212, a button 217 to set a check-in operation for a content corresponding to a music piece title selected in the field 213, a button 218 to set a check-in operation for all contents corresponding to content names displayed in the field 213, and a button 219 to cancel the check-in or check-out setting.

Even with the check-in or check-out setting made by using the buttons 216 to 219, however, the personal computer 1 will not execute the check-in or check-out operation.

When the button 215 is clicked after a check-in or check-out is set by using the buttons 216 to 219, the display/operation-instructive program 112 will make the content management program 111 execute the check-in or check-out. That is to say, when the button 215 is clicked, the display/operation-instructive program 112 will make, based on the check-in or check-out setting, the content management program 111 transmit a content, or a command to erase a predetermined content corresponding to the check-in setting (e.g., a command to erase a predetermined content stored in any of the portable devices 6-1 to 6-3), to any of the portable devices 6-1 to 6-3, and to update the usage rule stored in the usage rule file 162 corresponding to the content or command thus transmitted.

When the check-in or check-out is executed, the display/operation-instructive program 112 will respond to the transmitted content or command to update the history

data stored in the history data file 184. The history data includes information for identification of a content having been checked in or out or a date when the content has been checked in or out, and the name of a one of the portable devices 6-1 to 6-3 from which the content has been checked out.

Since the check-in or check-out can be set in a short time, the user can quickly know the status after execution of a check-in or check-out operation, whereby the number of times a time-taking check-in or check-out operation is done can be reduced to minimize the total time (including the setting and execution of a check-in or check-out operation) taken for the check-in or check-out procedure.

FIG. 6 shows an example of the window which the recording program 113 makes the display unit 20 display. Based on CD information received from the WWW server 5-2 for example, the recording program 113 will display a CD title such as “ACYNCHRONIZED” in a field 251. Also, based on CD information received from the WWW server 5-2, the recording program 113 will display an artist’s name such as “KUWAI” in a field 252.

Based on CD information received from the WWW server 5-2, the recording program 113 will display titles of music pieces such as “HEAT”, “PLANET”, “BLACK”, “SOUL”, etc. in a region of a field 253 where music piece titles are to be displayed. Similarly, the recording program 113 will display an artist’s name such as “KUWAI” is a region of the field 253 where artists’ names are to be displayed.

After receiving a predetermined CD information, the recording program 113

will store it into a predetermined directory in the HDD 21.

Upon reception of an instruction for acquisition of CD information via clicking of a button 254, the recording program 113 will first search the predetermined directory in the HDD 21. When the CD information is found stored in the directory, the recording program 113 will display a dialogue box (not shown) to prompt the user for selection of whether he or she is going to use the CD information stored in the directory.

When a button 256 displayed in the window displayed by the recording program 113 and which instructs to start recording of a content, is clicked, the recording program 113 will read a content from a CD set in the drive 22, and supply it along with the CD information to the content management program 111. The compression/expansion program 138 of the content management program 111 compresses the content supplied from the recording program 113 in a predetermined manner, and the encryption program 137 encrypts the compressed content. Also, the usage rule conversion program 139 generates a usage rule for the compressed and encrypted content.

The content management program 111 will supply the compressed and encrypted content along with the usage rule to the content data base 114.

The content data base 114 will generate a content file 161 and usage rule file 162 for the content received from the content management program 111, and store the content into the content file 161 and the usage rule into the usage rule file 162.

When the content and usage rule for the content are stored into the content data base 114, the content management program 111 will supply the CD information and usage rule received from the recording program 113 to the display/operation-instructive program 112.

The display/operation-instructive program 112 will a display data for storage into the display data file 182 according to the usage rule for the content stored in the content data base 114 by the recording and the CD information.

The window displayed by the recording program 113 has displayed therein a button 255 to automatically set whether any of the portable devices 6-1 to 6-3 is made to check out a content read from the CD when the content read from the CD is recorded into the content data base 114.

For example, when the button 255 is clicked, the recording program 113 will display a pull-down menu showing a list of the portable devices 6-1 to 6-3. When the user selects any of the portable devices 6-1 to 6-3 from the pull-down menu, the personal computer 1 will automatically check out the content recorded from the CD to any selected one of the portable devices 6-1 to 6-3. When the user selects "NOT CHECK OUT" from the pull-down menu, the personal computer 1 will not check out the content recorded from the CD.

Thus, when the content read from the CD is recorded into the content data base 114 with only the button 255 in the window displayed by the recording program 113 being set active, the personal computer 1 can make any pre-designated one of the

portable devices 6-1 to 6-3 check out the content read from the CD.

Referring now to FIG. 7, there is shown a flow chart of operations effected by the CPU 11 which executes the content management program 111, display/operation-instructive program 112, recording program 113 and content data base 114 in transferring a content played back from a CD set in the drive 22 to the HDD 21 and thus copying the content from the CD to the HDD 21. When the user operates the keyboard 18 or mouse 19 to supply to the CPU 11 via the interface 17, a command to transfer, for copying, a content played back from a CD (not shown) set in the drive 22, the recording program 113 will display, at step S11, a GUI (graphical user interface) shown in FIG. 6 for example, for selection of a content which is to be copied into the display unit 20 via the interface 17.

More specifically, the recording program 113 will read TOC (table of contents) of a CD set in the drive 22, acquire content information from the CD, and display it on the display unit 20. Alternatively, the recording program 113 will read ISRC (International Standard Recording Code) for each content included in the CD, acquire the content information, and display it on the display unit 20. Still alternatively, when the button 254 is clicked, the recording program 113 will access the WWW server 5-1 or 5-2 via the network 2, acquire the content information from the CD by the use of TOC, and display music piece titles corresponding to the content in the field 253.

Using GUI displayed on the display unit 20, the user operates the keyboard 18 or mouse 19, and clicks a check box for each of the music piece titles displayed in the

field 253 to select a content to be copied.

Next at step S12, the recording program 113 makes the usage rule management program 140 check the time limit data base stored in the HDD 21 (corresponding to the usage rule files 162-1 to 162-N in the content data base 114 shown in FIG. 4). The detail of this checking of the time limit data base will further be described later with reference to the flow chart shown in FIG. 8.

At step S31, the usage rule management program 140 cooperates with the CPU 32 of the adaptor 26 to compute a hash value of the entire time limit data base, and at step S32, it will compare the computed hash value with a previously saved one.

Note that when no data is recorded in the time limit data base, the usage rule management program 140 will not compute any hash value.

More particularly, the time limit data base is formed in the HDD 21, and stores, as information for management of contents recorded in the HDD 21, pairs of ISRC and copying date of a content having been recorded, as shown in FIG. 9. In the example shown in FIG. 9, ISRC and copying date area stored for each of three items 1 to 3. At step S38, a hash value of the entire time limit data base, based on the ISRCs and copying dates of all contents recorded in the time limit data base, is computed by the CPU 32 of the adaptor 26 and stored in the nonvolatile memory 34. The hash value is a value obtained by applying a hash function to the data. The hash function is generally a unidirectional function to map long data of a variable length with short data of a fixed length, and has such a nature that hash values will not easily conflict

with each other. The hash functions include SHA (secure hash algorithm), MD (message digest)5, etc. At step S31, the usage rule management program 140 compute a hash value as in the computation by the CPU 32. Then at step S32, the usage rule management program 140 will request the CPU 32 to read a hash value stored in the nonvolatile memory 34, and at step S31, it will compare the transferred hash value with the one it has computed.

At step S33, the usage rule management program 140 judges whether the hash value computed at step S31 coincides the hash value of the previous time limit data base stored in the nonvolatile memory 34. When no coincidence is found between the hash values, the usage rule management program 140 will determine that the time limit data base has been falsified or altered, and make the recording program 113 generate a message like “since time limit data base has been altered, no copying is possible” for example, and output the message to the display unit 20 via the interface 17 on which the message will be displayed. Hereafter, copying is inhibited. Namely, in this case, it is inhibited to play back the content recorded in the CD for copying to the HDD 21.

When the hash value computed at step S31 is found coincident with the preceding has value, the usage rule management program 140 goes to step S35 where it will make the recording program 113 acquire from the CD ISRC of a content designated at step S11 and selected as a one to be copied. If no ISRC is recorded in the CD, the usage rule management program 140 will make the recording program 113 read TOC data from the CD, and apply the hash function to the data to acquire a data

of an appropriate length such as 58 bits which is to be used for ISRC.

At step S36, the usage rule management program 140 judges whether the ISRC (selected content) acquired at step S35 is registered in the time limit data base (in FIG. 9). If the ISRC is not registered in the time limit data base, it means that the content has not yet been recorded in the HDD 21. So, the usage rule management program 140 goes to step S37 where it will register the ISRC of the content and present data into the time limit data base. Note that the usage rule management program 140 uses, as the present date, a value transferred from the CPU 32 and outputted from the RTC 35 of the adaptor 26. At step S38, the usage rule management program 140 reads data from the time limit data base at the time and transfer it to the CPU 32 of the adapter 26. The CPU 32 computes a hash value of transferred data and saves it in the nonvolatile memory 34. As in the above, the hash value this saved will be used as a previously saved hash value at step S32.

Next at step S39, the usage rule management program 140 will set a non-registration flag indicating that the selected content is not registered in the time limit data base. This flag is used at step S13 in FIG. 7 to judge whether the selected content is registered in the time limit data base.

If it has been determined at step S36 that the ISRC of the selected content is registered in the time limit data base, it means that the selected content is a one having been registered in the HDD 21 at least once. In this case, the usage rule management program 140 goes to step S40 where it will judge whether the present date (output



from the RTC 35 of the adaptor 26) is more than 48 hours from the date of the past registration of the selected content, registered in the time limit data base. When the present time is already more than 48 hours from the registration date, it means that the content has been recorded at least once in the HDD 21. However, since the present time is more than 48 hours from the date at the content was recorded, the content cannot substantially be copied in a large volume even if it is copied again. In this case, it is permitted to copy the content into the HDD 21. Then, the usage rule management program 140 will go to step S41 where it will change the date in the time limit data base from the date of the past registration to the present data (output from the RTC 35). Then, the usage rule management program 140 will return to step S38 where it will make the CPU 32 compute a hash value of the entire time limit data base and save it into the nonvolatile memory 34. At step S39, the usage rule management memory 140 will set a non-registration flag for that content.

On the other hand, if it is determined at step S40 that the present date is not more than 48 hours from the registration date, it is inhibited to copy the selected content into the HDD 21. In this case, the usage rule management program 140 will go to step S42 where it will set a registration flag for the selected content.

If the predetermined time is not judged at step S40 to have not elapsed, the content cannot newly be copied, so that copying the content in a large volume required for fraudulent sales or distribution for example is substantially disabled without unreasonable inhibition of the copying of the content for an ordinary, legal use. Note

that the criterion for the judgement, taken at step S40, is a time elapse of more than 48 hours but it is not limited to 48 hours. The criterion may be any time within a range of 12 hours to 168 hours for example.

As in the above, a flag indicating whether the selected content is registered in the HDD 21 is set through checking of the time limit data base.

Referring to FIG. 7 again, the description will further be made. At step S13, the copy management program 133 judges, based on the above-mentioned flag, that the selected content has been registered in the time limit data base. If the selected content has already been registered, the copy management program 133 will go to step S14 where it will make the recording program 113 display, on the display unit 20, a message like "This music piece cannot be copied since not more than 48 hours has elapsed since the music piece has been copied once" for example. Thus, the user can know the reason why the content cannot be copied to the HDD 21.

If it is determined at step S13 that the selected content has not yet been registered in the time limit data base, the copy management program 133 goes to step S15 where the recording program 113 will make the drive 22 read a content from the CD set in the drive 22. This content has a watermark code inserted therein at a predetermined position as shown in FIG. 10. The recording program 113 will extract the watermark code included in the content at step S16 and judge, at step S17, whether the watermark code indicates an inhibition of the content from being copied. If the watermark code indicates the copy inhibition, the

copy management program 133 will go to step S18 where it will make the recording program 113 display a message like “copying is inhibited” for example on the display unit 20 via the interface 17, and terminate the copying operation.

On the other hand, if it is judged at step S17 that the watermark code indicates no copy inhibition, the copy management program 133 goes to step S19 where the recording program 113 will make the compression/expansion program 138 compress the content by a software operation using a method such as ATRAC (Adaptive Transform Acoustic Coding)<sup>3</sup> (trade mark). At step S20, the recording program 113 will make the encryption program 137 encrypt the content by a method such as DES (Data Encryption Standard), FEAL (Fast Encipherment Algorithm ) or the like using an encryption key having been preset and stored in the memory 13. The encryption key may be a one formed based on a random number generated by a software operation or a random number generated by the CPU 32 of the adaptor 26. By encrypting the encryption key using the personal computer 1 and CPU 32 of the adaptor 26 as a hardware associated with the personal computer 1 in a cooperative combination, an encryption can be attained which will make it more difficult to decrypt the encrypted encryption key.

Next at step S21, the recording program 113 transfers an encrypted data to the content data base 114, gives a file name to the data and makes the HDD 21 save it as one file (as content file 161). Alternatively, the recording program 113 may give position information (e.g., a number of bytes from the top) as a part of one file to the

encrypted data before save into the HDD 21.

The data save may be done separately from or simultaneously with the aforementioned compression and encryption.

Further at step S22, the recording program 113 will make the encryption program 137 encrypt the encryption key with which the content has been encrypted, using a predetermined save key stored in the nonvolatile memory 34 and by the aforementioned DES method, FEAL method or the like, save the encrypted encryption key in the music data base in the HDD 21 (corresponding to the usage rule files 162-1 to 162-N of the content data base 114 shown in FIG. 4).

At step S23, the recording program 113 makes a set of saved information on the file, encrypted encryption key, information of the content, and elements of music piece title information supplied by the user via the GUI, and register it in the music data base in the HDD 21 (as the usage rule files 162-1 to 162-N). At step S24, the recording program 113 will make the CPU 32 compute a hash value of the entire music data base and save it into the nonvolatile memory 34.

In this way, the music data base as shown in FIG. 11 for example is registered into the HDD 21. In this example music data base, there are recorded a file name, encrypted encryption key, music piece title, play time length, playback conditions (start date, end date and playback limit), playback counter, playback accounting condition, copying condition (copies), copy counter and copying condition (SCMS) for each of items 1 to 3.

In the method defined by SDMI (Secure Digital Music Initiative) for example, a number of times a content copied from a CD can be checked out (check-out limit) is set to 3.

Since it is arranged that when a predetermined period of time elapses from copying of a content from a CD to the HDD 21, the content can be copied again, the content can be copied several times allowed only for private use by the user. On the other hand, if it is tried to copy the content a larger number of times than the allowed number for the private use by the user, for example, in a large volume, the copying will take a very long time and actually be impossible. Also even if the personal computer 1 has failed and the content recorded in the HDD 21 has been erased, the erased content can be copied again and recorded into the HDD 21 when a predetermined time elapses.

Also, the content of the time limit data base recorded into the HDD 21 can commonly be shared via the network 2.

In the above, there has been explained the example in which a copying date is stored correspondingly to ISRC. In addition to the ISRC, however, any other information (such as music piece title, album name or their combination) with which a content and CD can be identified may be used.

Next, move of a content from the HDD 21 to the flash memory 61 (e.g., memory stick (trade mark)) in the portable device 6 and content check-out, effected by the CPU 11 which executes the display/operation-instructive program 112 and

content management program 111 and CPU 52 which executes the main program, will be described herebelow with reference to the flow chart shown in FIGS. 12 to 14.

First, the content move will be described herebelow. At step S51, the move management program 134 makes the usage rule management program 140 compute the hash value of the entire music data base, and at step S52, it compares the computed hash value with a hash value having previously been computed by the CPU 32 and saved in the nonvolatile memory 34. When there is no coincidence between these hash values, the move management program 134 goes to step S53 where it will make the display/operation-instructive program 112 display a message like "Possibly music data base has been falsified or altered" on the display unit 20, and terminate the operation. These operations are similar to those effected at steps S31 to S34 in FIG. 8. In this case, the content move from the HDD 21 to the portable device 6 will not be done.

Next at step S54, the move management program 134 reads information on a content recorded in the music data base (included in the content data base 114) formed in the HDD 21, and makes the display/operation-instructive program 112 display the information as a selecting GUI on the display unit 20. The user clicks a music piece title (content name) and button 216 displayed in the field 212 in FIG. 5 to select the content to be moved from the HDD 21 to the portable device 6. Next at step S55, the move management program 134 examines the playback condition, copying condition, playback accounting condition, etc. for the content having been selected at step S54. This operation will further be described later with reference to the flow chart in FIG.

15.

Next at step S56, mutual authentication is made between the authentication program 141 of the personal computer 1 and CPU 53 of the portable device 6 and a communication key is shared between them.

For example, it is assumed here that the flash memory 61 (or EEPROM 68) of the portable device 6 has a master key KM stored in advance and the RAM 13 of the personal computer 1 (or a predetermined file in the HDD 21) has an individual key KP and ID stored in advance. The CPU 53 is supplied with the ID previously stored in the RAM 13 from the authentication program 141 and applies the hash function to that ID and its own master key MK to generate the same key as the individual key of the personal computer 1, stored in the RAM 13. Thus, the personal computer 1 and portable device 6 will share a common individual key which is used to generate a provisional communication key.

Alternately, an ID and master key KMP are stored in advance in the RAM 13 of the personal computer 1 and an ID and master key KMM are stored in advance in the flash memory 61 of the portable device 6. The RAM 13 sends its ID and master key to the flash memory 61 which will also send its ID and master key to the RAM 13, and the RAM 13 applies the hash function to the ID and master key received from the flash memory 61 while the latter will apply the hash function to the ID and master key received from the RAM 13. Thus, the RAM 13 generates an individual key for the flash memory 61 while the latter generates an individual key for the RAM 13. A

provisional communication key will further be generated from the individual key.

It should be noted that for the authentication method, the IOS (International Organization for Standardization) 9798-2 can be used for example.

When the mutual authentication is not correctly done, the operation is terminated. When the mutual authentication has successfully be done, the move management program 134 will make the content data base 114 read the file name of the selected content from the music data base at step S57, and reads a content having the file name (for example, the file name has been encrypted at step S20 in FIG. 7) from the HDD 21. At step S58, the move management program 134 converts the compression method (for the compression effected at step S19), encryption method (for the encryption effected at step S20), format (for example, that for the header), etc. having been used for the content being a digital data read at step S57 to those used in the portable device 6. The conversion will further be described later with reference to the flow chart in FIG. 17.

At step S59, the move management program 134 will make the PD driver 143 transfer the content converted at step S58 to the portable device 6 via the USB port 23. At step S60, the CPU 53 of the portable device 6 receives the transmitted content via the USB connector 56 and stores it as it is into the flash memory 61.

At step S61, the move management program 134 will further make the usage rule conversion program 139 convert the playback conditions (start date, end date, playback limit, etc.) for the selected content, registered in the music data base, to those



used in the portable device 6. At step S62, the move management program 134 will further make the usage rule conversion program 139 convert the SCMS information in the copying condition for the selected content, registered in the music data base, to a format managed by the portable device 6. Then at step S63, the move management program 134 makes the PD driver 143 transfer to the portable device 6 the playback condition having been converted at step S61 and SCMS information having converted at step S62. The CPU 53 of the portable device 6 saves the transferred playback condition and SCMS information into the flash memory 61.

At step S64, the move management program 134 makes the PD driver 143 transfer to the portable device 6 the playback condition, playback accounting condition, copying condition, etc. for the selected content, registered in the music data base, as in the format dealt with in the music data base by the CPU 11, and save them into the flash memory 61.

At step S65, the move management program 134 makes the content data base 114 reads the encrypted encryption key for the selected content from the music data base, and then at step S66, it will make the decryption program 142 decrypt the encryption key with the save key saved in the RAM 13, and the encryption program 137 encrypt the decrypted encryption key with the communication key. Then the move management program 134 will make the PD driver 143 transfer the encryption key encrypted with the communication key to the portable device 6.

At step S67, the CPU 53 of the portable device 6 will decrypt the encryption key

transferred from the personal computer 1 by the use of the common communication key generated by the mutual authentication, encrypt it using its own save key, correlate it with the already saved data, and save it into the flash memory 61.

Upon completion of the saving of the encryption key, the CPU 53 will inform, at step S68, the personal computer 1 that the encryption key has been saved. When receiving this information from the portable device 6 from the portable device 6, the move management program 134 of the personal computer 1 will make, at step S69, the content data base 114 delete the content file 161 corresponding to the content, and the set of the elements of the content (i.e., usage rule file 162) from the music data base. Thus, the content will be moved, not copied. At step S70, the move management program 134 transfers data in the music data base to the CPU 32 of the adaptor 26 and makes the CPU 32 compute the hash value of the entire music data base and save it into the nonvolatile memory 34. The hash value will be used as a previously saved one at step S52 having been described above.

Next, check-out of a content from the personal computer 1 to the portable device 6 will be described below. This operation is similar to the content move from the personal computer 1 to the portable device 6 as having been described in the above with reference to FIGS. 12 to 14. That is, the check-out operation is basically similar to the content move operation except that the check-out operation is executed in the personal computer 1 by the check-in/check-out management program 132, and that at step S69 in FIG. 14, the number of times the content checked out and recorded in the

music data base has been checked out (or can be checked out) is updated (in the content move, the content is deleted). Therefore, the check-out operation will not be described any longer.

Th CPU 11 which executes the content management program 111 checks the playback conditions, etc. for a content selected at step S55 in FIG. 12. This checking operation will be described below with reference to the flow chart in FIG. 15. At step S81, the movement management program 134 makes the content data base 114 read various conditions from the music data base. Then at step S82, the move management program 134 judges whether the copy counter in the conditions read at step S81 has already exceeded the copy limit. When the copy counter has already exceeded the copy limit, no further copy can be permitted, so the move management program 134 will go to step S83 where it will make the display/operation-instructive program 112 display a message like "Copy counter has already exceeded copy limit" on the display unit 20, and terminate the operation. If it is determined at step S82 that th copy counter has not exceeded the copy limit, the move management program 134 goes to step S84 where it will judge whether the present date is past the playback end date. The present date is a one outputted from the RTC 35 of the adaptor 26. With this operation, the user will not be able to use any present time of the personal computer 1, which is obtainable by intentionally correcting to a past one. The move management program 134 is supplied with the present time from the CPU 32, and makes by itself the judgement at step S84 or supplies, at step S81, the playback

conditions read from the music data base to the CPU 32 of the adaptor 26 and thus makes the CPU 32 do the judgement at step S84.

If the present date is past the playback end date, the move management program 134 goes to step S85 where it will make the content data base 114 erase the selected content from the HDD 21 and information on the selected content from the music data base. At step S86, the move management program 134 makes the CPU 32 compute the hash value of the entire music data base and save it into the nonvolatile memory 34. Here the operation is terminated. Therefore, no content will be moved in this case.

If it is determined at step S84 that the present date is not yet past the playback end data, the move management program 134 will go to step S87 where it will judge whether the playback-accounting condition (e.g., fee per playback) for the selected content is registered in the music data base. If the playback-accounting condition is found registered, the move management program 134 will make, at step S88, the PD driver 143 communicate with the portable device 6 to judge whether the portable device 6 has an accounting function. If the portable device 6 has no accounting function, the selected content cannot be transferred to the portable device 6. Therefore, the move management program 134 will make, at step S89, the display/operation-instructive program 112 display a message like "Destination has no accounting function" on the display unit 20, and terminate the operation.

If it is determined at step S87 that no playback-accounting condition is

registered or at step S88 that the portable device 6 has the accounting function, the move management program 134 goes to step S90 where it will judge whether other playback conditions such as playback limit are registered for the selected content. If the other playback conditions are found register, the move management program 134 goes to step S91 where it will judge whether the portable device 6 has a function to follow the playback conditions. If the portable device 6 has no such a function, the move management program 134 goes to step S92 where it will make the display/operation-instructive program 112 display a message like “Destination has no function to follow playback conditions” on the display unit 20, and terminate the operation.

If it is determined at step S90 that no playback conditions are registered, or if it is determined at step S91 that the portable device 6 has a function to follow the playback conditions, the checking of the playback conditions will be terminated, and the move management program 134 will return to step S56 in FIG. 12.

FIG. 16 shows an example of the playback condition managed (which can be followed) by the portable device 6. The playback conditions shown in FIG. 16 are stored in the EEPROM 68. In this example, a playback start date and end date are registered for each of contents for items 1 to 3. However, a playback limit is registered only for the item 2, not for the items 1 and 3. Therefore, when the content for the item 2 is taken as the selected content, it is possible to follow the playback limit as playback condition (a number of times a content can be played back), but when content for the

item 1 or 3 is taken as the selected content, it is not possible to follow the playback limit.

Next, format conversion effected at step S58 in FIG. 12 by the CPU 11 which executes the content management program 111, will be described in detail herebelow with reference to the flow chart shown in FIG. 17. At step S101, the move management program 134 checks the format of the selected content (e.g., a header including playback conditions, usage rule, copying conditions), recorded in the content data base 114. At step S102, the move management program 134 will check conditions settable in the destination (the portable device 6 in this case). Namely, the move management program 134 inquires the CPU 53 of the portable device 6 of such settable conditions and acquires a reply from the CPU 53. At step S103, the move management program 134 will determine, based on the conditions checked at step S102, ones, settable in the destination, of the conditions in the format registered in the music data base.

At step S104, the move management program 134 judges whether there are conditions settable in the destination. If there are no such conditions, the move management program 134 goes to step S105 where it will inhibit move of a content to the portable device 6. That is, in this case, since the conditions registered in the music data base cannot be followed by the portable device 6, content move to the portable device 6 is inhibited.

If it is determined at step S104 that such settable conditions exist, the move

management program 134 goes to step S106 where it will make the usage rule conversion program 139 convert the conditions to those in the function format of the destination (for example, conditions which are stored in the header when the selected content is transferred to the portable device 6). Then at step S107, the move management program 134 will set the converted conditions in the destination. As a result, the portable device 6 will be able to play back the content according to the set conditions (or following the conditions).

Next, copying of a content from the HDD 21 to the portable device 6, effected by the CPU 11 which executes the content management program 111 and CPU 53 which executes the main program, will be described herebelow with reference to the flow chart in FIGS. 18 to 20. The operations at steps S111 to S127 in FIGS. 18 to 20 are effected by the copy management program 133. These operations are similar to those at steps 51 to 67 for the content move from the HDD 21 to the portable device 6 as in FIGS. 12 to 14. Also in this case, the music data base is checked to see if it has been falsified or altered, and then the playback conditions for the selected content are checked with those recorded in the music data base. Further, after mutual authentication is made between the portable device 6 and personal computer 1, the content is transferred from the HDD 21 of the personal computer 1 to the flash memory 61 of the portable device 6, where it is saved. Thereafter at step S128, the copy management program 133 will increment the copy counter in the music data base by one. At step S129, the copy management program 133 makes the CPU 32 compute

the hash value of the entire music data base, and save it into the nonvolatile memory 34.

Next, content move from the portable device 6 to HDD 21 and check-in operation, effected by the CPU 11 which executes the content management program 111 and CPU 53 which executes the main program, will be described herebelow with reference to the flow chart in FIG. 21.

First, the content move will be explained. At step S161, the move management program 134 requests the CPU 53 of the portable device 6 to read content information stored in the flash memory 61. Upon reception of the request from the move management program 134, the CPU 53 will transmit to the personal computer 1 the content information stored in the flash memory 61. Based on the information, the move management program 134 makes the display unit 20 display GUI for selection of the contents stored in the flash memory 61. According to the GUI displayed on the display unit 20, the user will operate the keyboard 18 or mouse 19 to designate a content which is to be moved from the portable device 6 to the HDD 21 (content data base 114).

At step S162, the move management program 134 makes the authentication program 141 execute a mutual authentication with the CPU 53 to generate a communication key for common use between them. This operation is similar to that at step S56 in FIG. 12.

Next at step S163, the CPU 53 will read the encrypted selected content stored



in the flash memory 61, and transfers it to the personal computer 1. At step S164, the move management program 134 takes, as one file, the content transferred from the portable device 6 and gives a file name to it, and saves it into the content data base 114 (in the HDD 21). This save may be done with position information of the file (e.g., number of bytes from the top) given as a part of one file.

At step S165, the CPU 53 will read the encrypted encryption key for the selected content, recorded in the flash memory 61, decrypt it with its own save key, further encrypt it with the communication key, and then transfers it to the personal computer 1. The encryption key is a one having been saved in the flash memory 61 in the operation at step S67 in FIG. 14 for example.

Receiving the encryption key transferred from the portable device 6, the move management program 134 makes, at step S166, the decrypting program 142 decrypt the encryption key with the communication key, and the encryption key 137 encrypt it with its own save key. At step S167, the move management program 134 will make the content data base 114 register, into the music data base in the HDD 21, the content file name and content information saved at step S164, music piece name (content name) entered by the user via the GUI, the encryption key encrypted at step S166, etc. Then at step S168, the move management program 134 makes, via the CPU 32, the usage rule management program 140 compute the hash value of the entire music data base, and the nonvolatile memory 34 save it.

At step S169, the move management program 134 informs the portable device

6 that the encryption key has been saved, and requests it to delete the content. When requested from the personal computer 1 to delete the content, the CPU 53 will delete, at step S170, the content stored in the flash memory 61.

Next, the check-in of a content from the portable device 6 to the personal computer 1 will be described herebelow. The operations of content check-in from the portable device 6 to the personal computer is similar to the content move from the portable device 6 to the personal computer 1 as in FIG. 21. That is, the check-in operation is effected by the check-in/check-out management program 132 in the personal computer 1, and the operations at steps S162 to S166 in FIG. 21 are omitted. Also, the personal computer 1 will update, at step S167 in FIG. 21, the check-out limit, namely, a number of times the checked-in content can be checked out, recorded in the music data base, and after completion of the operation at step S170, operations basically similar to those in the content move except for the confirmation of the content file deletion will be effected. Therefore, the operations will not further be described.

Note that when the flash memory 61 of the portable device 6 is removable as a memory card, the personal computer 1 will effect the mutual authentication at step S162 in FIG. 21 in the check-in procedure.

Next, content copy from the portable device 6 to the HDD 21, effected by the CPU 11 which executes the content management program 111 and CPU 53 which executes the main program, will be described herebelow with reference to the flow

chart in FIG. 22. Operations at steps S181 to S188 in FIG. 22 are similar to those at steps S161 to S168 (in FIG. 21) in the content move from the portable device 6 to the HDD 21. That is, the copy is effected by the copy management program 133, and the copy operation is basically similar to the move operation except for the omission of the operations at steps S169 and S170 in FIG. 21. Therefore, the copy operation will not be described any further.

Next, copy of the content transferred from the EMD server 4 to the HDD 21, effected by the EMD server 4 and CPU 11 which executes the content management program 111, will be described below with reference to the flow chart in FIG. 23. When the user clicks the button 202 in FIG. 5 to make an instruction for access to the EMD server 4, the purchase program 144 makes, at step S201, the communications block 25 access the EMD server 4 via the network 2. In response to the access, the EMD server 4 will transfer information such as music piece number, title, information of a content held therein to the personal computer 1 via the network 2. Upon acquisition of the information, the purchase program 144 makes the display/operation-instructive program 112 display the information on the display unit 20 via the interface 17. Using the GUI displayed on the display unit 20, the user will designate, at step S202, a content he wants to copy. The designated information is transferred to the EMD server 4 via the network 2. At step S203, the purchase program 144 will effect a mutual authentication between itself and EMD server 4 via the network 2 to generate a communication key for common use between them.

The mutual authentication effected between the personal computer 1 and EMD server 4 may be done using a public key and private key defined in ISO 9798-3 for example. In this case, the personal computer 1 has its own private key and a public key for the EMD server 4 in advance, and the EMD server 4 has its own private key. The mutual authentication between the personal computer 1 and EMD server 4 is effected using these keys. The public key of the personal computer 1 may be made available to the personal computer 1 by transferring it from the EMD server 4 or a certificate having previously been distributed to the personal computer 1 for confirmation of the certificate by the EMD server 4. Further, at step S204, the purchase program 114 will make an accounting operation between itself and EMD server 4. The accounting operation will further be described later with reference to the flow chart in FIG. 24.

Next at step S205, the EMD server 4 transfers the encrypted content designated at step S202 to the personal computer 1 via the network 2. At this time, it transfers a time information at any time to the personal computer 1. At step S206, the purchase program 144 will give a file name to the transferred content and make the content data base 114 save it as one content file 161 into the HDD 21. At step S207, the EMD server 4 will further encrypt the encryption key for the content using the communication key common to itself and personal computer 1, generated at step S203, and transfer the encrypted encryption key to the personal computer 1.

At step S208, the purchase program 144 makes the decryption program 142 to

decrypt the encryption key transferred from the EMD server 4 using the communication key independently or in cooperation with the CPU 32 of the adaptor 26, and makes the encryption program 137 encrypt the decrypted encryption key with its own save key. At step S209, the purchase program 144 will make the content data base 114 register into the music data base in the HDD 21 a set of the file name of the content, content information, music piece title entered by the user, and encrypted encryption key. Further at step S210, the purchase program 144 makes the CPU 32 compute the hash value of the entire music data base, and save it into the nonvolatile memory 34.

Note that at step S205, the EMD server 4 will transmit the content along with the time data to the personal computer 1. The time data is transferred from the personal computer 1 to the adaptor 26. Upon reception of the time data transferred from the personal computer 1, the CPU 32 of the adaptor 26 corrects the time of the RTC 35 at step S211. Thus, based on the time information provided from an external device having been recognized as a correct device as the result of the mutual authentication, the time information of the RTC 35 of the adaptor 26 is corrected, so that the adaptor 26 can always keep correct time information.

Next, accounting effected at step S204 in FIG. 23 by the EMD server 4 and CPU 11 which executes the content management program 111, will be described herebelow with reference to the flow chart in FIG. 24. At step S221, the purchase program 144 read price information for the selected content designated at step S202

from price information transmitted from the EMD server 4 at step S201, and write it into an accounting log in the HDD 21. FIG. 25 shows an example of such accounting log. In this example, the user has copied items 1 to 3 from the EMD server 4, and the price for the items 1 and 2 is 50 yens while that for the item 3 is 60 yens. The hash value of this accounting log has been computed by the CPU 32, and registered in the nonvolatile memory 34.

Next at step S222, the purchase program 144 will read the accounting log written at step S221 from the HDD 21, and transfers it to the EMD server 4 via the network 2. At step S223, the EMD server 4 makes an accounting computation based on the accounting log transferred from the personal computer 1. That is, the EMD server 4 adds to a data base provided therein an accounting log transmitted from the user of the personal computer 1 to update the data base. At step S224, the EMD server 4 judges whether the accounting log is to be settle immediately. When it is determined that the accounting log is to be settled immediately, the EMD server 4 goes to step S225 where it will transfer to a settling server (not shown) a trade name, money amount, etc. necessary for the settlement. Then at step S226, the settling server will effect a settlement to the user of the personal computer 1. If it is determined at step S224 that the accounting log is not to be settled immediately, operations at steps S225 and S226 will be skipped over. Namely, these operations will be done periodically, for example, once a month.

Next, copying to the HDD 21 of a content having been played back by a CD

player (not shown) and entered from the IEC60958 terminal 24a of the audio input/output terminal 24, effected by the CPU 11 which executes the content management program 111, will be described below with reference to the flow chart shown in FIGS. 26 and 27. At step S241, the user connect the IEC60958 output terminal of the CD player to the IEC60958 terminal 24a of the audio input/output interface 24 of the personal computer 1. At step S242, the user operates the keyboard 18 or mouse 19 to enter the music piece title of a content to be copied from the CD player (or a number for the content). Then at step S243, the user operate a button on the CD player to start playing the CD player. In case a control signal transmission/reception line is connected between the CD player and personal computer 1, the user may operate the keyboard 18 or mouse 19 of the personal computer 1 to enter a playback start instruction for making the CD player start playing the CD.

When the CD player starts playing the CD, a content read out of the CD is transferred, at step S244, to the personal computer 1 via the IEC60958 terminal 24a. At step S245, the copy management program 133 reads SCMS (serial copy management system) data from the data entered via the IEC60958 terminal 24a. The SCMS data includes copying condition information such as inhibition of copy, permission of one copy, permission of free copy, etc. At step S246, the CPU 11 judges whether the SCMS data indicates inhibition of copy. If the SCMS data indicates the copy inhibition, the copy management program 133 goes to step S247 where it will make the display/operation-instructive program 112 display a message

like "Copy is inhibited" on the display unit 20, and terminate the copy operation. In this case, copy to the HDD 21 is inhibited.

At step S246, when it is determined by the CPU 11 that the SCMS information read at step S245 does not indicate any copy inhibition, the copy management program 133 will go to step S248 where it reads a watermark code, and at step S249, it will judge whether the watermark code indicates inhibition of copy. When the watermark code indicates the copy inhibition, the copy management program 133 goes to step S247 where it will make the display/operation-instructive program 112 display a predetermined message as in the above and terminate the copy operation.

If it is determined at step S249 that the watermark code does not indicate any copy inhibition, the copy management program 133 goes to step S250 where it will check the time limit data base. If the selected content is found already been registered as the result of the checking of the time limit data base, the operation is ended with operations at steps S251 and S252. These operations are similar to those at steps S13 and S14 shown in FIG. 7.

If the selected content is not a content having not yet been registered in the HDD 21, it will be registered at steps S253 to S258. The operations at steps S253 to S258 are similar to those at steps S19 to S24 in FIG. 7 except that the SCMS information supplied from the IEC60958 terminal 24a is also registered in the music data base at step S257. Therefore, the operations will not be described any further,

Next, output (playback) of a content from the HDD 21 to the IEC60958



terminal 24a, effected by the CPU 11 which executes the content management program 111, will be described herebelow with reference to the flow chart shown in FIGS. 28 and 29. At steps S271 to S273, the hash value of the entire music data base is computed as at steps S111 to S113 in FIG. 18, and it is judged whether the hash value coincides with a one previously saved to check whether the music data base has been falsified or altered. If it is determined that the music data base has not been falsified, the display/operation-instructive program 112 goes to step S274 where it will make, via the content management program 111, the content data base 114 access the music data base in the HDD 21, read information on music pieces registered in the music data base, and display it on the display unit 20. Watching the display, the user operates the keyboard 18 or mouse 19 in an appropriate manner to select a content which the user wants to play back. At step S275, the display/operation-instructive program 112 checks the playback conditions for the selected content. The check of the playback conditions will further be described later with reference to the flow chart in FIG. 30.

Next at step S276, the display/operation-instructive program 112 makes, via the content management program 111, the content data base 114 read from the music data base an encryption key for the content selected at step S274, and the decryption program 142 decrypt the encryption key with the save key. At step S277, the display/operation-instructive program 112 makes, via the content management program 111, the content data base 114 reads from the music data base SCMS

information of the selected content, and determines SCMS information to be outputted from the IEC60958 terminal 24a according to the rule for the SCMS system. For example, when the number of times a content can be played back is limited (namely, as a playback limit), the playback counter is incremented by one. The playback count thus incremented is taken as new SCMS information. At step S278, the display/operation-instructive program 112 will further make, via the content management program 111, the content data base 114 read ISRC for the selected content from the music data base.

Next at step S279, the display/operation-instructive program 112 will make, via the content management program 111, the content data base 114 read the file name from the selected content from the music data base, and then read the content from the HDD 21 based on the file name. Further the display/operation-instructive program 112 will further make, via the content management program 111, the content data base 114 read an encryption key for the content from the music data base, and the decryption program 142 decrypt the encryption key with the save key and then decrypt the encrypted content with the decrypted encryption key. The compression/expansion program 138 will further decrypt (expand) the compression code for the content. At step S280, the display/operation-instructive program 112 makes the driver 117 output, at the IEC60958 24a, the decrypted content (digital data) read at step S279 along with the SCMS information determined at step S277 and ISRC information read at step S278 according to the IEC60958 rule. Furthermore, the display/operation-instructive

program 112 will put a program such as real player (trade mark; not shown) into run to convert the content being a digital data to an analog data and output it at the analog output terminal of the audio input/output interface 24.

At step S281, the display/operation-instructive program 112 will make, via the content management program 111, the content data base 114 increment the playback counter in the music data base by one. At step S282, it is judged whether the selected content has playback accounting conditions added thereto. If the selected content has the playback accounting conditions added thereto, the display/operation-instructive program 112 goes to step S283 where it will make, via the content management program 111, the content data base 114 write a corresponding fee into the accounting log. At step S284, the display/operation-instructive program 112 makes, via the usage rule management program 140, the CPU 32 compute the hash value of the entire music data base and store it into the nonvolatile memory 34. If it is determined at step S282 that the selected content has no playback accounting conditions added thereto, the display/operation-instructive program 112 will skip over operations at steps S283 and S284.

Next, checking of playback conditions at step S275 in FIG. 28, effected by the CPU 11 which executes the content management program 111, will be described below in detail with reference to the flow chart shown in FIG. 30. At step S301, the display/operation-instructive program 112 will make, via the content management program 111, the content data base 114 read various conditions in the music data base.

At step S302, the usage rule management program 140 judges whether the playback count in the conditions read from the music data base is over the playback limit. If the playback count is over the playback limit, the usage rule management program 140 goes to step S303 where it will make, via the content management program 111, the content data base 114 delete the selected content from the HDD 21 and the information on the selected content from the music data base. At step S304, the display/operation-instructive program 112 will further make, via the usage rule management program 140, the CPU 32 compute a new hash value of the music data base and save it into the nonvolatile memory 34. In this case, the playback (output) is inhibited.

If it is determined at step S302 that the playback count is not over the playback limit, the usage rule management program 140 goes to step S305 where it will judge whether the playback end date is past the present date. If the playback end date is past the present date, the display/operation-instructive program 112 will make, at step S303, the usage rule management program 140 delete the selected date from the HDD 21 and also from the music data base as in the above. At step S304, a new hash value of the music data base is computed and saved. Also in this case, the playback (output) is inhibited.

If it is determined at step S305 that the playback end date is not past the present date, the CPU 32 goes to step S306 where it will judge whether the selected content has the playback accounting conditions added thereto. If the selected content has the

playback accounting conditions added thereto, the display/operation-instructive program 112 goes to step S307 where it will make the display unit 20 display a message of the addition of the playback accounting conditions and a fee. If it is determined at step S306 that the selected content has no playback accounting conditions added thereto, operation at step S307 will be skipped over.

Next, playback (output) of a content from the HDD 21 via the portable device 6, effected by the CPU 11 which executes the content management program 111 and CPU 53 which executes the main program, will be described below with reference to the flow chart shown in FIGS. 31 and 32. At steps S321 to S325, the music data base is checked for any falsification or alteration, the selected content is designated, and playback conditions for the selected content are checked. These operations are similar to those at steps S271 to S275 in FIG. 28, and so will not be described any longer.

At step S326, a mutual authentication is effected between the portable device 6 and personal computer 1 to generate a communication key for common use between them. At step S327, the display/operation-instructive program 112 instructs the portable device 6 to play back an encrypted content which is going to be supplied. At step S328, the display/operation-instructive program 112 will make, via the content management program 111, the content data base 114 read S324 from the music data base the designated file name of the content selected at step, and the content having the file name from the HDD 21. At step S329, the display/operation-instructive program 112 will make the content management program 111 convert the content

compression method, encryption method and format to those used in the portable device 6. Further at step S330, the display/operation-instructive program 112 makes the encryption program 137 encrypt the content converted at step S329 with the communication key, and transfer it to the portable device 6.

At step S331, the CPU 53 of the portable device 6 responds to an instruction transferred from the personal computer 1 at step S327 to decrypt each transferred data with the communication key and play it back. At step S332, the display/operation-instructive program 112 will make, via the content data base 114, the content management program 111 increment the playback counter in the music data base by one. Further at step S333, the display/operation-instructive program 112 will judge whether the selected content has playback accounting conditions added thereto. If the selected content has the playback accounting conditions added thereto, the display/operation-instructive program 112 makes, via the content management program 111 at step S334, the content data base 114 write a fee for the playback into an accounting log. At step S335, the display/operation-instructive program 112 will make the CPU 32 compute and save a new hash value of the entire music data. If the selected content has no such playback conditions added thereto, operations at steps S334 and S335 will be skipped over.

The present invention provides various arrangements for prevention of a content from fraudulently being copied. For example, the program to operate the CPU 11 is a so-called tamper-resistant software of which the executing sequence varies at each

operation of the CPU 11.

Further, the function of the CPU 11 is partially shared by the adaptor 26 as a hardware so that both the CPU 11 and adaptor 26 work together to execute a variety of operations. Thus, a higher data security is ensured.

For example, the hash value of the music data base is not saved in the music data base itself as in the above, but in the nonvolatile memory 34 of the adaptor 26. Namely, in the comparison with the hash value previously saved as at steps S32 and S33 in FIG. 8 for example, the previous hash value for comparison is stored in the nonvolatile memory 34. Thereby, all the records including a content saved in the HDD 21 can be backed up before they are copied or moved to any other recording medium. After a content saved in the HDD 21 is copied or moved from the HDD 21 to any other recording medium, a content included in the records backed up in the HDD 21 can be restored again, whereby it is made possible to prevent the content from being copied or moved substantially limitlessly disregarding the usage rule.

For example, when contents A and B are saved in the HDD 21 as shown in FIG. 33, hash values for the contents A and B are saved in the nonvolatile memory 34. It is assumed here that in this condition, a part or all of recorded data including the contents A and B in the HDD 21 are backed up in other recording medium 271. When the content A in the HDD 21 is moved to a further recording medium 272 after that, only the content B will remain in the content recorded in the HDD 21, so that the hash value in the nonvolatile memory 34 is also changed to a one for the content B.

When a part or all of the recorded data in the HDD 21, backed up in the recording medium 271, is restored in the HDD 21 thereafter and the contents A and B are saved again into the HDD 21, a hash value computed from information of the content B will be found stored in the nonvolatile memory 34 while the hash value computed from the information of the contents A and B will not be found stored in the nonvolatile memory 34. Thus, the hash value computed based on the contents A and B stored on the HDD 21 will not coincident with the previous hash value stored in the nonvolatile memory 34, and it will be detected that the music data base has been falsified. As a result, the usage of the contents A and B saved in the HDD 21 will be limited thereafter.

Further, as having been described in the above, the adaptor 26 incorporates the RTC 35. The RTC 35 has the time information corrected based on a time data transferred from any other device (e.g., EMD server 4) which could correctly be authenticated. A present date outputted from the RTC 35, not any one managed by the personal computer 1, is used. Therefore, the user will not be able to intentionally edit the present data in the personal computer 1 to any past time for avoiding that the present time is judged to be past the playback end date included in the playback conditions.

Also the adaptor 26 is designed to decrypt a transferred encrypted program according to a program previously stored in the ROM 36 and execute the program, so that a higher data security can be assured. This will further be described below with



reference to the flow chart shown in FIG. 34.

More specifically, when the personal computer 1 is going to execute a predetermined operation for the adaptor 26, it will encrypt, at step S351, a program to be executed by the adaptor 26 with an encryption key previously stored in the RAM 13, and transfer it to the adaptor 26. The RAM 13 of the adaptor 26 has previously stored therein a program transferred from the personal computer 1 and intended to decrypt and execute the encrypted program. The CPU 32 follows this program stored in the RAM 36 to decrypt at step S352 the encrypted program stored in the RAM 36. The CPU 32 will develop the decrypted program to the RAM 33 at step S313, and execute it at step S354.

As having been described in the foregoing, when the adaptor 26 is made to compute a hash value of the music data base in the HDD 21 for example, the CPU 11 of the personal computer 1 will encrypt the data in the music data base with the encryption key and transfer it to the CPU 32 of the adaptor 26. The CPU 32 will apply the hash function to the transferred data in the music data base to compute a hash value. The hash value thus computed is stored into the nonvolatile memory 34. Alternatively, the CPU 32 compares the hash value with a previous one having been stored in advance, and transfer the result of computation to the CPU 11 of the personal computer 1.

FIG. 35 shows in detail the internal construction of the adaptor 26. The adaptor 26 is formed as a semiconductor IC. As shown in FIG. 35, the adaptor 26 includes, in

addition to the interface 31, CPU 32, RAM 33, nonvolatile memory 34, RTC 35, ROM 36 as shown in FIG. 2, a RAM controller 301 to control write and read to and from the RAM 33, and a logic circuit 302 provided for use to output directly from the adaptor 26 an encrypted content having been decrypted as in the above.

The blocks from the interface 31 to ROM 36, RAM controller 301 and logic circuit 302 are integrally built in the semiconductor IC in such a manner that they cannot be disassembled from outside.

Further, a crystal oscillator 311 is provided to generate a clock for a reference in execution of various operations by the adaptor 6. Also an oscillator circuit 312 is provided to put the RTC 35 into operation. The adaptor 26 further includes a battery 313 which supplies backup power to the oscillator circuit 312, nonvolatile memory 34 and RTC 35. In addition, the component circuits of the adaptor 26 are supplied with a power from a power supply circuit 321 of the personal computer 1.

The nonvolatile memory 34 may be composed of an erasable ROM. In case it is composed of a RAM backed up by the backup power from the battery 313, however, a protective aluminum layer 351 may be formed on the nonvolatile memory 34 and a power source pattern 352 to supply the nonvolatile memory 34 with the power from the battery 313 be formed flush with the protective aluminum layer 351, as shown in FIGS. 36A and 36B for example. Thus, if the user tries to remove the protective aluminum layer 351 in order to alter the nonvolatile memory 34, the power source pattern 352 flush with the nonvolatile memory 34 will also be removed, power supply

to the nonvolatile memory 34 will be shut off, and data stored in the memory 34 will be erased. In this way, the tamper-resistance can further be improved.

Further, the adaptor 26 has wires 401-1 to 401-3 provided to write or read data to or from the nonvolatile memory 34. The wires 401-1 to 401-3 are formed to vertically overlap each other as shown in FIG. 37. Thus, for reading data from the lowest wire 401-3, the wires 401-1 and 401-2 above the wire 401-3 have to be removed. Thus, data cannot be read simultaneously from the wires 401-1 to 401-3.

Also, the wires 401-1 to 401-3 of the nonvolatile memory 34 may be formed redundantly. For example, when the wires 401-1 to 401-3 formed inside the nonvolatile memory 34 are used to connect elements such as transistors forming the nonvolatile memory 34, paths for them are formed not linearly even if the elements can be connected linearly by wires but they are formed to have a predetermined length. Thus, the wires 401-1 to 401-3 will be longer than required and have a larger parasitic capacitance than that which would be when the wires are a minimum necessary length.

The dedicated circuit (incorporated in the adaptor 26 being a semiconductor IC) designed for data read from the nonvolatile memory 34 can normally read data stored in the nonvolatile memory 34 when an impedance matching its parasitic capacitance is set. However, when a probe is connected to the wires 401-1 to 401-3 in order to read data from the nonvolatile memory 34, the combination of the parasitic capacitance and probe capacitance will result in an influence due to which data cannot normally be read from the nonvolatile memory 34.

In the foregoing, the portable device 6 has been used to explain the recording medium, but it should be noted that the present invention is applicable in data move or copy to any other recording medium.

The content may be image and other data in addition to the musical sound data such as music or audio data.

As having been described in the foregoing, the present invention is advantageous as will be described below:

(1) According to the present invention, data is encrypted for recording into the HDD 21 and the encryption key is encrypted with the save key for recording into the HDD 21. Thus, even if a content recorded in the HDD 21 is copied, it cannot be decrypted so that it cannot be copied in large volume for distribution.

(2) According to the present invention, when a predetermined music piece is copied once, its title and recording date are registered in the music data base in order to prevent the music piece from being copied for a predetermined period of time (48 hours in the aforementioned example). Thus, the number of times the music piece can be copied can be limited to prevent the music piece from being copied in a large volume for distribution.

Further according to the present invention, each time the data base is updated, the hash data of the data is computed and saved. Thus, it is easy to prevent the data base from being falsified or altered.

(3) According to the present invention, once a content is passed to an

external device, a corresponding one in the HDD 21 is erased. Thus, the content being an original digital data will not remain in the HDD 21 and it cannot be copied in a large amount for distribution.

(4) According to the present invention, the music data base is provided in the HDD 21 to check the hash value of the entire music data base at each time. Thus, even if a content in the HDD 21 is backed up before being moved and the backed-up data is restored into the HDD 21 just after the content is moved, it is possible to positively erase the data in the content source.

(5) According to the present invention, before data is passed from the personal computer 1 to an external device, a mutual authentication is done between the personal computer 1 and external device. Thus, the data can be prevented from being passed to any wrong device.

(6) According to the present invention, before data is passed from any external device to the personal computer 1, it is confirmed by a mutual authentication between the external device and personal computer 1 whether the software of the personal computer 1 is a legal one. Thus, it is possible to prevent a content from being passed to any wrong software.

(7) According to the present invention, ISRC is used to identify a music piece, and if no ISRC is available, TOC is used. Thus, even when no ISRC is available for a music piece, it is possible to identify the music piece.

(8) According to the present invention, a predetermined part of the

software function of the personal computer 1 is performed by the adaptor 26 provided as an external device connected to the personal computer 1. Thus, just with analysis of the software of the personal computer 1, it is not possible to know how the software as a whole works. Therefore, it is impossible to add any intended function to the software by falsifying or altering.

Note that the operations which are to be conducted by the adaptor 26 may be done by the CPU 11 according to a security program. In this case, save keys having the same value are generated by the content management program 111 when a save key becomes necessary, for example. Similarly, the hash value is concealed for saving by the content management program 111.

Also, when an operation which is to be conducted by the adaptor 26 is done by the CPU 11 according to the security program, the personal computer 1 downloads a present time data from a predetermined server (e.g., EMD registration server 3) connected to the network 2 instead of a present time supplied from the RTC 35 of the adaptor 26, and effects a judgement based on the present time data. Also, the personal computer 1 may be designed, for this purpose, to store present times at predetermined time intervals and display an error when a time before a stored present time is set, thereby accepting any intentional time setting.

The aforementioned series of operations may be conducted by the hardware and also by the software. In the latter case, a program forming the software will be installed from a program storage medium into a computer incorporated in a dedicated

hardware or a general-purpose personal computer, for example, in which a variety of functions can be performed according to various programs installed therein.

As shown in FIG. 2, the program storage medium which stores a program installed in a computer and made executable by the computer includes the magnetic disc 41 (including a floppy disc), optical disc 42 (CD-ROM (= compact disc-read-only memory)), DVD (digital versatile disc), magneto-optical disc 43 (MD (= mini-disc)), package medium formed from the semiconductor memory 44, ROM 12 in which the program is stored provisionally or permanently, or HDD 21. The program is stored into the program storage medium via the interface such as the communications block 25 as necessary by using the network 2 such as a local area network (LAN) or Internet, cable or radio communications media such as digital satellite broadcasting.

Note that the operations of describing a program for storage into the program storage medium, referred to herein, include those which are done time-serially along a described sequence and those which are not effected time-serially but in parallel or individually.

Also note that the "system" referred to herein means an assembly of a plurality of devices.

As in the foregoing, the information processing apparatus and method, and the program storage medium, according to the present invention, are adapted to control accumulation or read of content data into or from the storage means by a controlling means made of a software on the basis of results of operations of the program

executing means provided in the hardware, thereby permitting to positively prevent data from fraudulently being copied by analysis and falsification of the software.

01  
02  
03  
04  
05  
06  
07  
08  
09  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28  
29  
30  
31  
32  
33  
34  
35  
36  
37  
38  
39  
40  
41  
42  
43  
44  
45  
46  
47  
48  
49  
50  
51  
52  
53  
54  
55  
56  
57  
58  
59  
60  
61  
62  
63  
64  
65  
66  
67  
68  
69  
70  
71  
72  
73  
74  
75  
76  
77  
78  
79  
80  
81  
82  
83  
84  
85  
86  
87  
88  
89  
90  
91  
92  
93  
94  
95  
96  
97  
98  
99  
100  
101  
102  
103  
104  
105  
106  
107  
108  
109  
110  
111  
112  
113  
114  
115  
116  
117  
118  
119  
120  
121  
122  
123  
124  
125  
126  
127  
128  
129  
130  
131  
132  
133  
134  
135  
136  
137  
138  
139  
140  
141  
142  
143  
144  
145  
146  
147  
148  
149  
150  
151  
152  
153  
154  
155  
156  
157  
158  
159  
160  
161  
162  
163  
164  
165  
166  
167  
168  
169  
170  
171  
172  
173  
174  
175  
176  
177  
178  
179  
180  
181  
182  
183  
184  
185  
186  
187  
188  
189  
190  
191  
192  
193  
194  
195  
196  
197  
198  
199  
200  
201  
202  
203  
204  
205  
206  
207  
208  
209  
210  
211  
212  
213  
214  
215  
216  
217  
218  
219  
220  
221  
222  
223  
224  
225  
226  
227  
228  
229  
230  
231  
232  
233  
234  
235  
236  
237  
238  
239  
240  
241  
242  
243  
244  
245  
246  
247  
248  
249  
250  
251  
252  
253  
254  
255  
256  
257  
258  
259  
260  
261  
262  
263  
264  
265  
266  
267  
268  
269  
270  
271  
272  
273  
274  
275  
276  
277  
278  
279  
280  
281  
282  
283  
284  
285  
286  
287  
288  
289  
290  
291  
292  
293  
294  
295  
296  
297  
298  
299  
300  
301  
302  
303  
304  
305  
306  
307  
308  
309  
310  
311  
312  
313  
314  
315  
316  
317  
318  
319  
320  
321  
322  
323  
324  
325  
326  
327  
328  
329  
330  
331  
332  
333  
334  
335  
336  
337  
338  
339  
340  
341  
342  
343  
344  
345  
346  
347  
348  
349  
350  
351  
352  
353  
354  
355  
356  
357  
358  
359  
360  
361  
362  
363  
364  
365  
366  
367  
368  
369  
370  
371  
372  
373  
374  
375  
376  
377  
378  
379  
380  
381  
382  
383  
384  
385  
386  
387  
388  
389  
390  
391  
392  
393  
394  
395  
396  
397  
398  
399  
400  
401  
402  
403  
404  
405  
406  
407  
408  
409  
410  
411  
412  
413  
414  
415  
416  
417  
418  
419  
420  
421  
422  
423  
424  
425  
426  
427  
428  
429  
430  
431  
432  
433  
434  
435  
436  
437  
438  
439  
440  
441  
442  
443  
444  
445  
446  
447  
448  
449  
450  
451  
452  
453  
454  
455  
456  
457  
458  
459  
460  
461  
462  
463  
464  
465  
466  
467  
468  
469  
470  
471  
472  
473  
474  
475  
476  
477  
478  
479  
480  
481  
482  
483  
484  
485  
486  
487  
488  
489  
490  
491  
492  
493  
494  
495  
496  
497  
498  
499  
500  
501  
502  
503  
504  
505  
506  
507  
508  
509  
510  
511  
512  
513  
514  
515  
516  
517  
518  
519  
520  
521  
522  
523  
524  
525  
526  
527  
528  
529  
530  
531  
532  
533  
534  
535  
536  
537  
538  
539  
540  
541  
542  
543  
544  
545  
546  
547  
548  
549  
550  
551  
552  
553  
554  
555  
556  
557  
558  
559  
560  
561  
562  
563  
564  
565  
566  
567  
568  
569  
570  
571  
572  
573  
574  
575  
576  
577  
578  
579  
580  
581  
582  
583  
584  
585  
586  
587  
588  
589  
590  
591  
592  
593  
594  
595  
596  
597  
598  
599  
600  
601  
602  
603  
604  
605  
606  
607  
608  
609  
610  
611  
612  
613  
614  
615  
616  
617  
618  
619  
620  
621  
622  
623  
624  
625  
626  
627  
628  
629  
630  
631  
632  
633  
634  
635  
636  
637  
638  
639  
640  
641  
642  
643  
644  
645  
646  
647  
648  
649  
650  
651  
652  
653  
654  
655  
656  
657  
658  
659  
660  
661  
662  
663  
664  
665  
666  
667  
668  
669  
670  
671  
672  
673  
674  
675  
676  
677  
678  
679  
680  
681  
682  
683  
684  
685  
686  
687  
688  
689  
690  
691  
692  
693  
694  
695  
696  
697  
698  
699  
700  
701  
702  
703  
704  
705  
706  
707  
708  
709  
710  
711  
712  
713  
714  
715  
716  
717  
718  
719  
720  
721  
722  
723  
724  
725  
726  
727  
728  
729  
730  
731  
732  
733  
734  
735  
736  
737  
738  
739  
740  
741  
742  
743  
744  
745  
746  
747  
748  
749  
750  
751  
752  
753  
754  
755  
756  
757  
758  
759  
760  
761  
762  
763  
764  
765  
766  
767  
768  
769  
770  
771  
772  
773  
774  
775  
776  
777  
778  
779  
780  
781  
782  
783  
784  
785  
786  
787  
788  
789  
790  
791  
792  
793  
794  
795  
796  
797  
798  
799  
800  
801  
802  
803  
804  
805  
806  
807  
808  
809  
810  
811  
812  
813  
814  
815  
816  
817  
818  
819  
820  
821  
822  
823  
824  
825  
826  
827  
828  
829  
830  
831  
832  
833  
834  
835  
836  
837  
838  
839  
840  
841  
842  
843  
844  
845  
846  
847  
848  
849  
850  
851  
852  
853  
854  
855  
856  
857  
858  
859  
860  
861  
862  
863  
864  
865  
866  
867  
868  
869  
870  
871  
872  
873  
874  
875  
876  
877  
878  
879  
880  
881  
882  
883  
884  
885  
886  
887  
888  
889  
890  
891  
892  
893  
894  
895  
896  
897  
898  
899  
900  
901  
902  
903  
904  
905  
906  
907  
908  
909  
910  
911  
912  
913  
914  
915  
916  
917  
918  
919  
920  
921  
922  
923  
924  
925  
926  
927  
928  
929  
930  
931  
932  
933  
934  
935  
936  
937  
938  
939  
940  
941  
942  
943  
944  
945  
946  
947  
948  
949  
950  
951  
952  
953  
954  
955  
956  
957  
958  
959  
960  
961  
962  
963  
964  
965  
966  
967  
968  
969  
970  
971  
972  
973  
974  
975  
976  
977  
978  
979  
980  
981  
982  
983  
984  
985  
986  
987  
988  
989  
990  
991  
992  
993  
994  
995  
996  
997  
998  
999  
1000  
1001  
1002  
1003  
1004  
1005  
1006  
1007  
1008  
1009  
1010  
1011  
1012  
1013  
1014  
1015  
1016  
1017  
1018  
1019  
1020  
1021  
1022  
1023  
1024  
1025  
1026  
1027  
1028  
1029  
1030  
1031  
1032  
1033  
1034  
1035  
1036  
1037  
1038  
1039  
1040  
1041  
1042  
1043  
1044  
1045  
1046  
1047  
1048  
1049  
1050  
1051  
1052  
1053  
1054  
1055  
1056  
1057  
1058  
1059  
1060  
1061  
1062  
1063  
1064  
1065  
1066  
1067  
1068  
1069  
1070  
1071  
1072  
1073  
1074  
1075  
1076  
1077  
1078  
1079  
1080  
1081  
1082  
1083  
1084  
1085  
1086  
1087  
1088  
1089  
1090  
1091  
1092  
1093  
1094  
1095  
1096  
1097  
1098  
1099  
1100  
1101  
1102  
1103  
1104  
1105  
1106  
1107  
1108  
1109  
1110  
1111  
1112  
1113  
1114  
1115  
1116  
1117  
1118  
1119  
1120  
1121  
1122  
1123  
1124  
1125  
1126  
1127  
1128  
1129  
1130  
1131  
1132  
1133  
1134  
1135  
1136  
1137  
1138  
1139  
1140  
1141  
1142  
1143  
1144  
1145  
1146  
1147  
1148  
1149  
1150  
1151  
1152  
1153  
1154  
1155  
1156  
1157  
1158  
1159  
1160  
1161  
1162  
1163  
1164  
1165  
1166  
1167  
1168  
1169  
1170  
1171  
1172  
1173  
1174  
1175  
1176  
1177  
1178  
1179  
1180  
1181  
1182  
1183  
1184  
1185  
1186  
1187  
1188  
1189  
1190  
1191  
1192  
1193  
1194  
1195  
1196  
1197  
1198  
1199  
1200  
1201  
1202  
1203  
1204  
1205  
1206  
1207  
1208  
1209  
1210  
1211  
1212  
1213  
1214  
1215  
1216  
1217  
1218  
1219  
1220  
1221  
1222  
1223  
1224  
1225  
1226  
1227  
1228  
1229  
1230  
1231  
1232  
1233  
1234  
1235  
1236  
1237  
1238  
1239  
1240  
1241  
1242  
1243  
1244  
1245  
1246  
1247  
1248  
1249  
1250  
1251  
1252  
1253  
1254  
1255  
1256  
1257  
1258  
1259  
1260  
1261  
1262  
1263  
1264  
1265  
1266  
1267  
1268  
1269  
1270  
1271  
1272  
1273  
1274  
1275  
1276  
1277  
1278  
1279  
1280  
1281  
1282  
1283  
1284  
1285  
1286  
1287  
1288  
1289  
1290  
1291  
1292  
1293  
1294  
1295  
1296  
1297  
1298  
1299  
1300  
1301  
1302  
1303  
1304  
1305  
1306  
1307  
1308  
1309  
1310  
1311  
1312  
1313  
1314  
1315  
1316  
1317  
1318  
1319  
1320  
1321  
1322  
1323  
1324  
1325  
1326  
1327  
1328  
1329  
1330  
1331  
1332  
1333  
1334  
1335  
1336  
1337  
1338  
1339  
1340  
1341  
1342  
1343  
1344  
1345  
1346  
1347  
1348  
1349  
1350  
1351  
1352  
1353  
1354  
1355  
1356  
1357  
1358  
1359  
1360  
1361  
1362  
1363  
1364  
1365  
1366  
1367  
1368  
1369  
1370  
1371  
1372  
1373  
1374  
1375  
1376  
1377  
1378  
1379  
1380  
1381  
1382  
1383  
1384  
1385  
1386  
1387  
1388  
1389  
1390  
1391  
1392  
1393  
1394  
1395  
1396  
1397  
1398  
1399  
1400  
1401  
1402  
1403  
1404  
1405  
1406  
1407  
1408  
1409  
1410  
1411  
1412  
1413  
1414  
1415  
1416  
1417  
1418  
1419  
1420  
1421  
1422  
1423  
1424  
1425  
1426  
1427  
1428  
1429  
1430  
1431  
1432  
1433  
1434  
1435  
1436  
1437  
1438  
1439  
1440  
1441  
1442  
1443  
1444  
1445  
1446  
1447  
1448  
1449  
1450  
1451  
1452  
1453  
1454  
1455  
1456  
1457  
1458  
1459  
1460  
1461  
1462  
1463  
1464  
1465  
1466  
1467  
1468  
1469  
1470  
1471  
1472  
1473  
1474  
1475  
1476  
1477  
1478  
1479  
1480  
1481  
1482  
1483  
1484  
1485  
1486  
1487  
1488  
1489  
1490  
1491  
1492  
1493  
1494  
1495  
1496  
1497  
1498  
1499  
1500  
1501  
1502  
1503  
1504  
1505  
1506  
1507  
1508  
1509  
1510  
1511  
1512  
1513  
1514  
1515  
1516  
1517  
1518  
1519  
1520  
1521  
1522  
1523  
1524  
1525  
1526  
1527  
1528  
1529  
1530  
1531  
1532  
1533  
1534  
1535  
1536  
1537  
1538  
1539  
1540  
1541  
1542  
1543  
1544  
1545  
1546  
1547  
1548  
1549  
1550  
1551  
1552  
1553  
1554  
1555  
1556  
1557  
1558  
1559  
1560  
1561  
1562  
1563  
1564  
1565  
1566  
1567  
1568  
1569  
1570  
1571  
1572  
1573  
1574  
1575  
1576  
1577  
1578  
1579  
1580  
1581  
1582  
1583  
1584  
1585  
1586  
1587  
1588  
1589  
1590  
1591  
1592  
1593  
1594  
1595  
1596  
1597  
1598  
1599  
1600  
1601  
1602  
1603  
1604  
1605  
1606  
1607  
1608  
1609  
1610  
1611  
1612  
1613  
1614  
1615  
1616  
1617  
1618  
1619  
1620  
1621  
1622  
1623  
1624  
1625  
1626  
1627  
1628  
1629  
1630  
1631  
1632  
1633  
1634  
1635  
1636  
1637  
1638  
1639  
1640  
1641  
1642  
1643  
1644  
1645  
1646  
1647  
1648  
1649  
1650  
1651  
1652  
1653  
1654  
1655  
1656  
1657  
1658  
1659  
1660  
1661  
1662  
1663  
1664  
1665  
1666  
1667  
1668  
1669  
1670  
1671  
1672  
1673  
1674  
1675  
1676  
1677  
1678  
1679  
1680  
1681  
1682  
1683  
1684  
1685  
1686  
1687  
1688  
1689  
1690  
1691  
1692  
1693  
1694  
1695  
1696  
1697  
1698  
1699  
1700  
1701  
1702  
1703  
1704  
1705  
1706  
1707  
1708  
1709  
1710  
1711  
1712  
1713  
1714  
1715  
1716  
1717  
1718  
1719  
1720  
1721  
1722  
1723  
1724  
1725  
1726  
1727  
1728  
1729  
1730  
1731  
1732  
1733  
1734  
1735  
1736  
1737  
1738  
1739  
1740  
1741  
1742  
1743  
1744  
1745  
1746  
1747  
1748  
1749  
1750  
1751  
1752  
1753  
1754  
1755  
1756  
1757  
1758  
1759  
1760  
1761  
1762  
1763  
1764  
1765  
1766  
1767  
1768  
1769  
1770  
1771  
1772  
1773  
1774  
1775  
1776  
1777  
1778  
1779  
1780  
1781  
1782  
1783  
1784  
1785  
1786  
1787  
1788  
1789  
1790  
1791  
1792  
1793  
1794  
1795  
1796  
1797  
1798  
1799  
1800  
1801  
1802  
1803  
1804  
1805  
1806  
1807  
1808  
1809  
1810  
1811  
1812  
1813  
1814  
1815  
1816  
1817  
1818  
1819  
1820  
1821  
1822  
1823  
1824  
1825  
1826  
1827  
1828  
1829  
1830  
1831  
1832  
1833  
1834  
1835  
1836  
1837  
1838  
1839  
1840  
1841  
1842  
1843  
1844  
1845  
1846  
1847  
1848  
1849  
1850  
1851  
1852  
1853  
1854  
1855  
1856  
1857  
1858  
1859  
1860  
1861  
1862  
1863  
1864  
1865  
1866  
1867  
1868  
1869  
1870  
1871  
1872  
1873  
1874  
1875  
1876  
1877  
1878  
1879  
1880  
1881  
1882  
1883  
1884  
1885  
1886  
1887  
1888  
1889  
1890  
1891  
1892  
1893  
1894  
1895  
1896  
1897  
1898  
1899  
1900  
1901  
1902  
1903  
1904  
1905  
1906  
1907  
1908  
1909  
1910  
1911  
1912  
1913  
1914  
1915  
1916  
1917  
1918  
1919  
1920  
1921  
1922  
1923  
1924  
1925  
1926  
1927  
1928  
1929  
1930  
1931  
1932  
1933  
1934  
1935  
1936  
1937  
1938  
1939  
1940  
1941  
1942  
1943  
1944  
1945  
1946  
1947  
1948  
1949  
1950  
1951  
1952  
1953  
1954  
1955  
1956  
1957  
1958  
1959  
1960  
1961  
1962  
1963  
1964  
1965  
1966  
1967  
1968  
1969  
1970  
1971  
1972  
1973  
1974  
1975  
1976  
1977  
1978  
1979  
1980  
1981  
1982  
1983  
1984  
1985  
1986  
1987  
1988  
1989  
1990  
1991  
1992  
1993  
1994  
1995  
1996  
1997  
1998  
1999  
2000  
2001  
2002  
2003  
2004  
2005  
2006  
2007  
2008  
2009  
2010  
2011  
2012  
2013  
2014  
2015  
2016  
2017  
2018  
2019  
2020  
2021  
2022  
2023  
2024  
2025  
2026  
2027  
2028  
2029  
2030  
2031  
2032  
2033  
2034  
2035  
2036  
2037  
2038  
2039  
2040  
2041  
2042  
2043  
2044  
2045  
2046  
2047  
2048  
2049  
2050  
2051  
2052  
2053  
2054  
2055  
2056  
2057  
2058  
2059  
2060  
2061  
2062  
2063  
2064  
2065  
2066  
2067  
2068  
2069  
2070  
2071  
2072  
2073  
2074  
2075  
2076  
2077  
2078  
2079  
2080  
2081  
2082  
2083  
2084  
2085  
2086  
2087  
2088  
2089  
2090  
2091  
2092  
2093  
2094  
2095  
2096  
2097  
2098  
2099  
2100  
2101  
2102  
2103  
2104  
2105  
2106  
2107  
2108  
2109  
2110  
2111  
2112  
2113  
2114  
2115  
2116  
2117  
2118  
2119  
2120  
2121  
2122  
2123  
2124  
2125  
2126  
2127  
2128  
2129  
2130  
2131  
2132  
2133  
2134  
2135  
2136  
2137  
2138  
2139  
2140  
2141  
2142  
2143  
2144  
2145  
2146  
2147  
2148  
2149  
2150  
2151  
2152  
2153  
2154  
2155  
2156  
2157  
2158  
2159  
2160  
2161  
2162  
2163  
2164  
2165  
2166  
2167  
2168  
2169  
2170  
2171  
2172  
2173  
2174  
2175  
2176  
2177  
2178  
2179  
2180  
2181  
2182  
2183  
2184  
2185  
2186  
2187  
2188  
2189  
2190  
2191  
2192  
2193  
2194  
2195  
2196  
2197  
2198  
2199  
2200  
2201  
2202  
2203  
2204  
2205  
2206  
2207  
2208  
2209  
2210  
2211  
2212  
2213  
2214  
2215  
2216  
2217  
2218  
2219  
2220  
2221  
2222  
2223  
2224  
2225  
2226  
2227  
222



## CLAIMS

1. An information processing apparatus comprising:
  - means for storing content data;
  - a controlling means having a software which controls storage or read of the content data into or from the content data storage means; and
  - means provided in a hardware independent of the controlling means to decrypt and execute an encrypted program supplied from the controlling means and supply the result of the program execution to the controlling means;
  - the controlling means controlling the content data storage or read to or from the content data storage means based on the program execution result supplied from the program executing means.
1. The apparatus as set forth in Claim 1, wherein:
  - the content data storage means stores also management information with which the content data stored in itself is managed; and
  - the controlling means makes the program executing means execute a predetermined computation based on the management information.
3. The apparatus as set forth in Claim 1, wherein:
  - the controlling means is a CPU;
  - the content data storing means is a hard disc; and
  - the program executing means is a CPU incorporated in a semiconductor IC

001-19

other than a one in which the CPU as the controlling means is built.

4. (Amended) An information processing apparatus comprising:

a storage medium for storing content data and content management information for the content data;

a process controller formed from a software to control storage or read of content data into or from the storage medium; and

a program execution controller provided in a semiconductor chip independent of the process controller and which is supplied with an encrypted program from the process controller, decrypts the program and supplies the result of the program execution to the process controller;

the process controller controlling storage or read of the content data into or from the storage medium based on the result of the program execution by the program execution controller; and

the program execution controller being adapted so that its internal operations cannot be confirmed from outside the semiconductor chip, and making a computation for checking any falsification made to the content management information.

5. (Amended) An information processing method for use in an information processing apparatus comprising:

means for storing content data;

a controlling means having a software which controls storage or read of the content data into or from the content data storage means; and

ant. 19

means provided in a hardware independent of the controlling means to decrypt and execute an encrypted program supplied from the controlling means and supply the result of the program execution to the controlling means;

the method comprising a step of:

controlling storage or read of content data into or from the content data storage means based on the result of the program execution by a program executing means.

6. (Amended) An information processing method for use in an information processing apparatus comprising:

a storage medium for storing content data and content management information for the content data;

a process controller formed from a software to control storage or read of content data into or from the storage medium; and

a program execution controller provided in a semiconductor chip independent of the process controller and which is supplied with an encrypted program from the process controller, decrypts the program and supplies the result of the program execution to the process controller;

the process controller controlling storage or read of the content data into or from the storage medium based on the result of the program execution by the program execution controller; and

the program execution controller being adapted so that its internal operations cannot be confirmed from outside the semiconductor chip, and making a computation

Oct. 14

for checking any falsification made to the content management information.

7. (Amended) A program storage medium for use in an information processing apparatus comprising:

means for storing content data;

a controlling means having a software which controls storage or read of the content data into or from the content data storage means; and

means provided in a hardware independent of the controlling means to decrypt and execute an encrypted program supplied from the controlling means and supply the result of the program execution to the controlling means;

the controlling means having recorded therein a computer-readable program comprising a step of controlling storage or read of the content data into or from the content data storing means based on the result of the program execution by the program executing means.

8. (Amended) An information processing apparatus comprising:

means for inputting content data;

means for storing the content data supplied from the input means;

means for compressing the content data stored in the content data storing means in a predetermined manner;

means for encrypting the data stored in the content data storing means in a predetermined manner; and

means for controlling storage or read, into or from the content data storing

Art. 19

means, of the content data compressed by the compressing means and encrypted by the encrypted means.

9. (Amended) The apparatus as set forth in Claim 8, wherein the compressing means compresses, or the encrypting means encrypts, different data supplied from the input means in the same manner.

10. (Amended) The apparatus as set forth in Claim 8, wherein the compressing means compresses, or encrypting means encrypts, different data supplied from the input means in different manners, respectively, and takes a predetermined common compressing or encrypting manner for outputting the data read from the content data storing means to a predetermined apparatus.

11. (Amended) An information processing apparatus comprising:

an interface via which content data is supplied from a predetermined recording medium or server;

a storage medium for storing content data supplied via the interface;

a compression program for compressing content data for storage into the storage medium in a predetermined manner;

an encryption program for encrypting the content data for storage into the storage medium in a predetermined manner; and

a controller for controlling storage or read, into or from the storage medium, the content data having been compressed by the compression program and encrypted by the encryption program;

Oct 19

the compression program compressing, or the encryption program encrypting, content data supplied via the interface and having been processed in different manners, in the same manner or different manners, respectively, for storage into the storage medium, and converting, when reading from the storage medium the content data having been compressed or encrypted in the different manners, respectively, for delivery to a predetermined portable device, the content data so that they can be compressed or encrypted in a common manner to both this apparatus and portable device.

12. (Amended) An information processing method comprising the steps of:  
inputting data;  
storing the data supplied from the data input step;  
compressing the data stored at the data storing step in a predetermined manner;  
encrypting the data stored at the data storing step in a predetermined manner;  
and  
controlling storage or read of the data compressed at the compressing step and encrypted at the encrypting step.
13. (Amended) An information processing method comprising the steps of:  
inputting content data from a predetermined recording medium or server;  
storing content data supplied at the data input step;  
compressing the content data stored at the data storing step in a predetermined manner;

Oct. 19

encrypting the content data stored at the compressing step in a predetermined manner; and

controlling storage or read, into or from the storage medium, the content data having been compressed at the compressing step and encrypted at the encrypting step;

the compressing step compressing, or the encryption step encrypting, content data supplied at the data input step and having been processed in different manners, in the same manner or different manners, respectively, for storage into the storage medium, and converting, when reading from the storage medium the content data having been compressed or encrypted in the different manners, respectively, for delivery to a predetermined portable device, the content data so that they can be compressed or encrypted in a common manner to both this apparatus and portable device.

14. (Amended) A program storage medium having recorded therein a program intended for execution by an information processing apparatus and readable by a computer, the program comprising the steps of:

inputting data;

storing the data supplied from the data input step;

compressing the data stored at the data storing step in a predetermined manner;

encrypting the data stored at the data storing step in a predetermined manner;

and

controlling storage or read of the data compressed at the compressing step and

Art. 19

encrypted at the encrypting step.

15. (Amended) An information processing apparatus comprising:

means for inputting content data;

means for storing the content data supplied from the content data input means;

means for holding management information for the content data stored in the content data storing means;

means for making a predetermined computation based on the management information held in the management information holding means; and

means for controlling the usage of the content data stored in the content data storing means according to a result of a comparison made between the result of the computation made by the computing means and that of the past computation which is stored in the content data storing means.

16. (Amended) The apparatus as set forth in Claim 15, wherein the computing means makes the computation using a hash function as the management information.

17. (Amended) The apparatus as set forth in Claim 15, wherein the data is music data and the management information includes identification information for identification of the music data.

18. (Amended) An information processing apparatus comprising:

an interface for input of content data and identification information of the content data;

a storage medium for storing content data supplied via the interface;

Oct. 19



a first memory for holding, as a usage rule file, the identification information of the content data stored in the storage medium;

a management program for making a computation with the hash function applied to the identification information held in the first memory;

a second memory for storing the result of the computation by the management program; and

a controller for comparing the result of the computation by the management program with the past computation result stored in the second memory to inhibit, when there is no coincidence between the computation results, copy or move of the content data stored in the storage medium.

19. (Amended) An information processing method comprising the steps of:
  - inputting data;
  - storing the data supplied at the data input step;
  - holding management information for the data stored at the data storing step;
  - making a predetermined computation based on the management information held at the management information holding step;
  - storing the result of the computation made at the computing step; and
  - comparing the result of the computation made at the computing step with a past computation result stored at the data storing step to control the usage of the data stored at the data storing step.

20. (Amended) An information processing method comprising steps of:

*Art. 19*

inputting content data and identification information of the content data;  
storing the content data supplied at the input step into a storage medium;  
holding, as a usage rule file, the identification information of the content data stored at the storing step;

making a computation with the hash function applied to the identification information held at the holding step;

storing the result of the computation made at the computing step; and

comparing the result of the computation at the computing step with a past computation result stored at the storing step to inhibit, when there is no coincidence between the computation results, copy or move of the content data stored in the storage medium.

21. (Amended) A program storage medium having recorded therein a program intended for execution by an information processing apparatus and readable by a computer, the program comprising the steps of:

inputting data;

storing the data supplied from the data input step;

holding management information for the data stored at the data storing step;

making a predetermined computation based on the management information held at the management information holding step;

storing the result of the computation made at the computing step; and

controlling the usage of the data stored at the data storing step according to a

Oct 19

result of a comparison made between the result of the computation made at the computing step and that of the past computation stored at the data storing step.

22. (Amended) An information processing apparatus comprising:

means for transmitting and receiving data to and from other apparatus;

means for holding a predetermined lock key and save key;

authenticating means which uses the lock key held in the holding means when transmitting and receiving data to and from the other apparatus to make a mutual authentication with the other apparatus to generate a communication key;

means for encrypting the communication key with the save key; and

means for storing the data received by the data transmitting and receiving means and having been encrypted with the communication key correspondingly to the communication key encrypted by the encrypting means.

23. (Amended) The apparatus as set forth in Claim 22, further comprising:

an encryption key decrypting means for decrypting the communication key stored in the storing means using the save key; and

means for decrypting the data stored in the storing means.

24. (Added) An information processing apparatus comprising:

an interface via which data is transferred between the apparatus and a portable device or server connected to the apparatus;

a memory for holding predetermined master key and save key;

an authentication program which uses, when the data is to be transferred to or

Oct 19

from the portable device or server, the master key stored in the memory to make a mutual authentication with the portable device or server to generate a communication key;

an encryption decryption program to decrypt, with the communication key, an encryption key with which the content data transmitted from the portable device or server has been encrypted and encrypt the encryption key with the save key;

a storage medium for storing the content data received via the interface and encrypted with the communication key in correspondence with the encryption key encrypted with the save key;

an encryption key decryption program to decrypt, with the save key, the encryption key stored in the storage medium; and

a data decryption program to decrypt content data stored in the storage medium with the encryption key decrypted by the encryption decryption program.

25. (Added) An information processing method comprising the steps of:

transmitting and receiving data to and from other apparatus;

holding a predetermined lock key and save key;

using the lock key held at the holding step when transmitting and receiving data to and from the other apparatus to make a mutual authentication with the other apparatus to generate a communication key;

encrypting the communication key with the save key; and

storing the data received at the data transmitting and receiving step and having

Oct 19

been encrypted with the communication key correspondingly to the communication key encrypted at the encrypting step.

26. (Added) An information processing method comprising the steps of:  
transferring data between the apparatus and a portable device or server connected to the apparatus;

holding predetermined master key and save key;

mutually authenticating with the portable device or server, when data is to be transferred to or from the portable device or server, using the master key held at the holding step to generate a communication key;

decrypting, with the communication key, an encryption key with which the content data transmitted from the portable device or server has been encrypted and encrypting the encryption key with the save key;

storing the content data received via the interface and encrypted with the communication key in correspondence with the encryption key encrypted with the save key;

decrypting, with the save key, the encryption key stored in the storage medium at the storing step; and

decrypting content data stored in the storage medium with the encryption key decrypted at the encryption decrypting step.

27. (Added) A program storage medium having recorded therein a program intended for execution by an information processing apparatus and readable by a

Ans. 19

computer, the program comprising the steps of:

transmitting and receiving data to and from other apparatus;

holding a predetermined lock key and save key;

using the lock key held at the holding step when transmitting and receiving data to and from the other apparatus to make a mutual authentication with the other apparatus to generate a communication key;

encrypting the communication key with the save key; and

storing the data received at the data transmitting and receiving step and having been encrypted with the communication key correspondingly to the communication key encrypted at the encrypting step.

28. (Added) An information processing apparatus comprising:

means for storing data;

means for holding the usage rule for the data stored in the data storing means;

means for judging whether or not, when moving the data stored in the data storing means to other apparatus, the usage rule for the data stored in the data storing means is reproducible by the other apparatus; and

means for moving, based on the result of the judgment by the judging means, the data stored in the data storing means to the other apparatus along with the usage rule for the data stored in the data storing means, which is held in the holding means.

29. (Added) The apparatus as set forth in Claim 28, wherein the usage rule for the data include:

*Art-19*

playback limiting condition;  
 playback accounting condition; or  
 copy limiting condition.

30. (Added) An information processing apparatus comprising:  
 a storage device to store content data;  
 a memory to hold a usage rule for the content data stored in the storage device;  
 and

a move management program to judge, when the content data stored in the storage device is to be moved to a portable device, whether the portable device meets the usage rule;

move of the content data stored in the storage device to the portable device being inhibited when it is determined as the result of the judgment by the move management program that the portable device does not meet the usage rule.

31. (Added) The apparatus as set forth in Claim 30, wherein the move includes copy, move or check-out, and the usage rule includes playback limiting condition, playback accounting condition or copy limiting condition.

32. (Added) An information processing method comprising steps of:  
 storing data;  
 holding the usage rule for the data stored at the data storing step;  
 judging whether or not, when moving the data stored at the data storing step to other apparatus, the usage rule for the data stored at the data storing step is

Art. 19

reproducible by the other apparatus; and

moving, based on the result of the judgment at the judging step, the data stored in the data storing means to the other apparatus along with the usage rule for the data stored at the data storing step, which is held at the holding step.

33. (Added) An information processing method comprising steps of:

storing content data into a storage device;

holding in a memory a usage rule for the content data stored in the storage device; and

judging, when the content data stored in the storage device is to be moved to a portable device, whether the portable device meets the usage rule;

inhibiting move of the content data stored in the storage device to the portable device when it is determined that the portable device does not meet the usage rule.

34. (Added) The method as set forth in Claim 33, wherein the move includes copy, move or check-out, and the usage rule includes playback limiting condition, playback accounting condition or copy limiting condition.

35. (Added) A program storage medium having recorded therein a program intended for execution by an information processing apparatus and readable by a computer, the program comprising steps of:

storing data;

holding the usage rule for the data stored at the data storing step;

judging whether or not, when moving the data stored at the data storing step to

*Art. 14*



other apparatus, the usage rule for the data stored at the data storing step is reproducible by the other apparatus; and

moving, based on the result of the judgment at the judging step, the data stored in the data storing means to the other apparatus along with the usage rule for the data stored at the data storing step, which is held at the holding step.

103/8

Ans. 19

## ABSTRACT

The CPU 11 of the personal computer 1 controls the CPU 32 of the adaptor 26 made of a semiconductor IC to compute a hash value of a content-managing music data base recorded in the HDD 21 and store it into the nonvolatile memory 34. When playing back a content recorded in the HDD 21, the CPU 11 computes the hash value of the music data base recorded in the HDD 21, compares it with hash values stored cumulatively in the nonvolatile memory 34, and controls the playback of the content from the HDD 21 based on the result of the comparison.

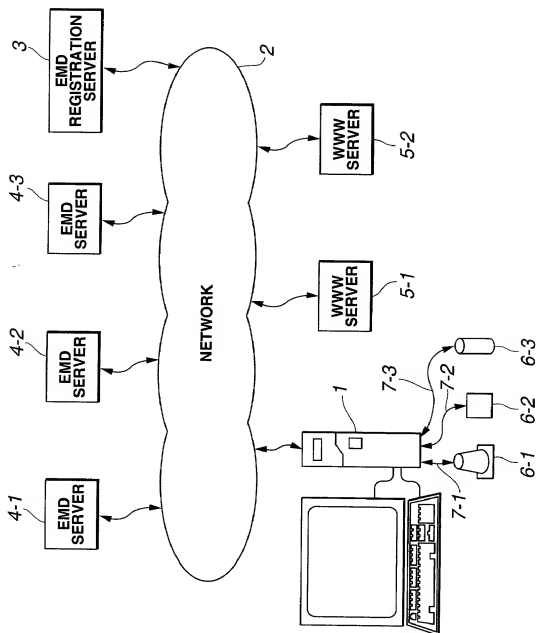


FIG.1

2/36

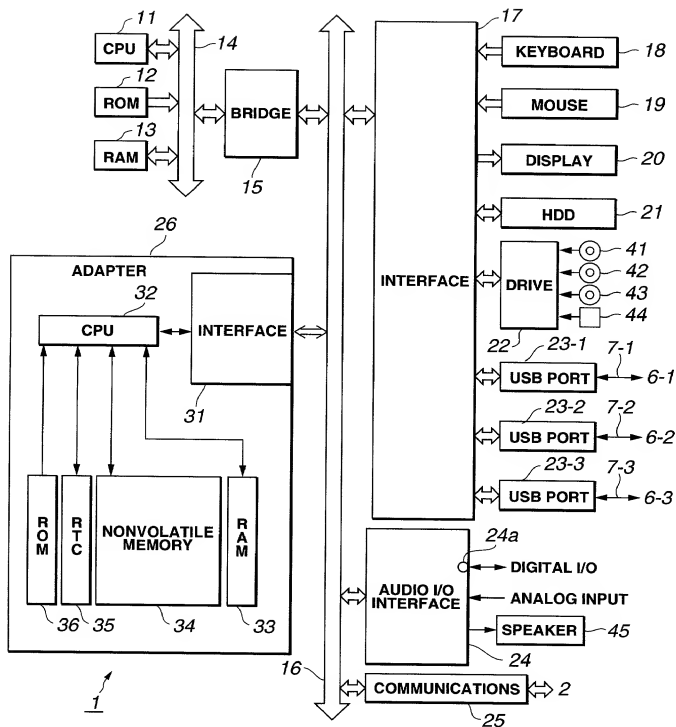


FIG.2

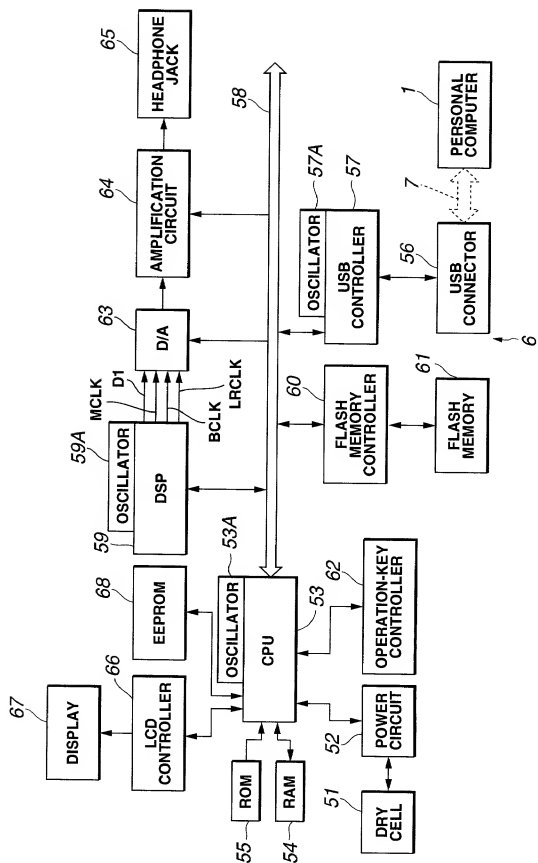


FIG. 3

4/36

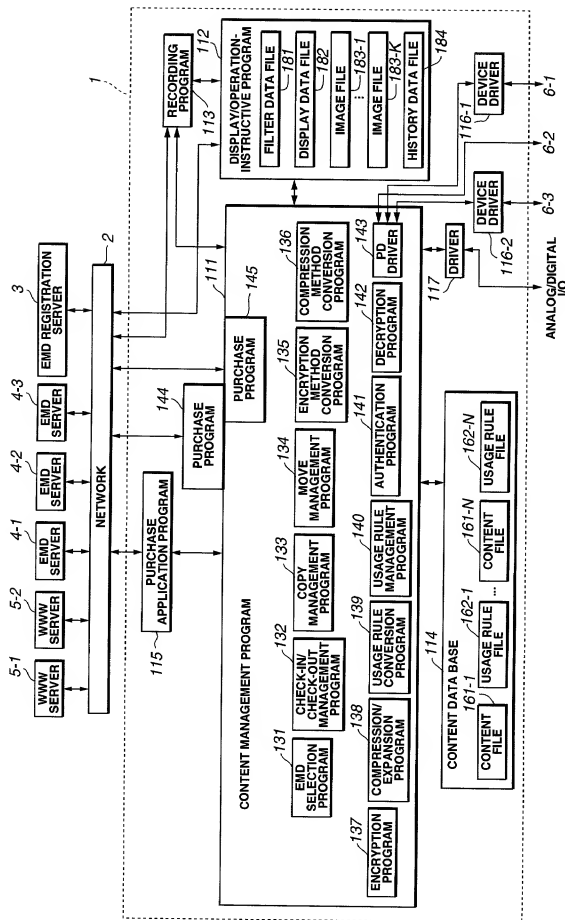


FIG.4

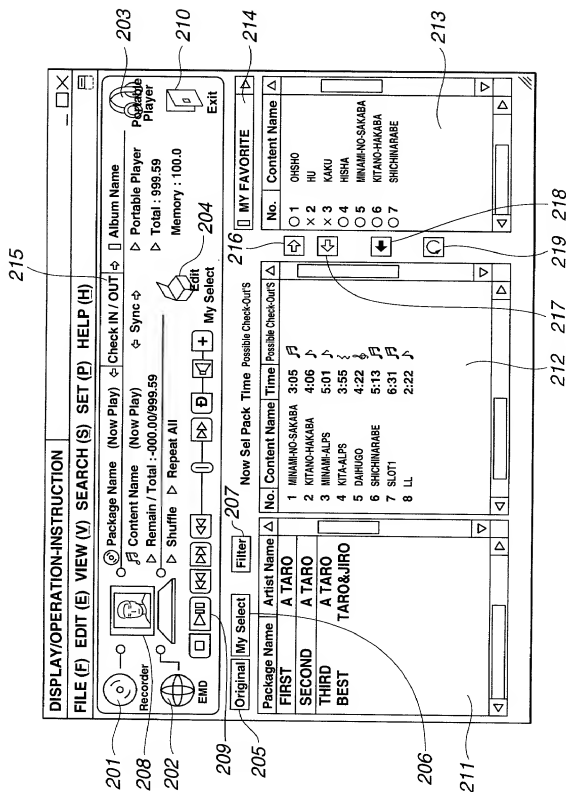


FIG. 5

6/36

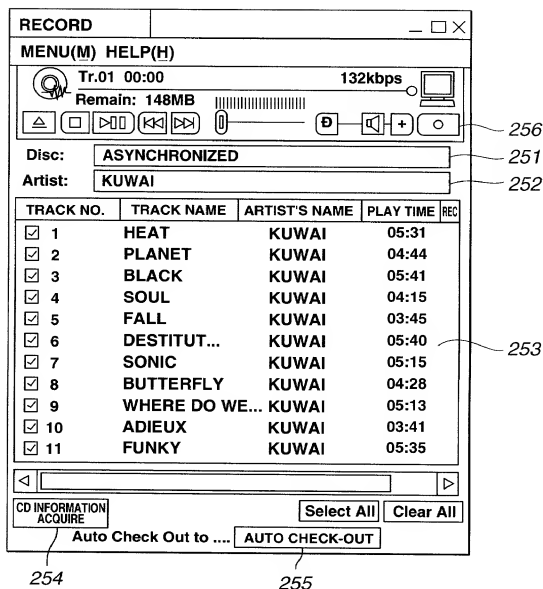


FIG.6



7/36

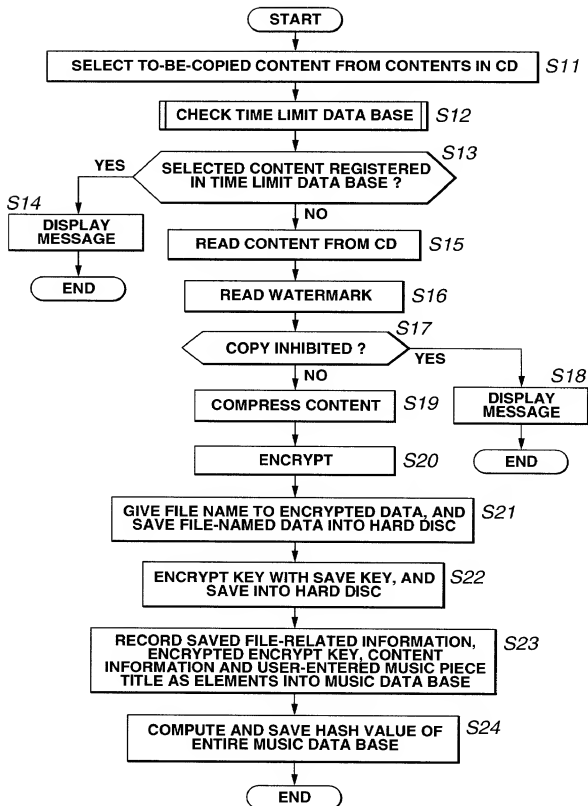


FIG.7

8/36

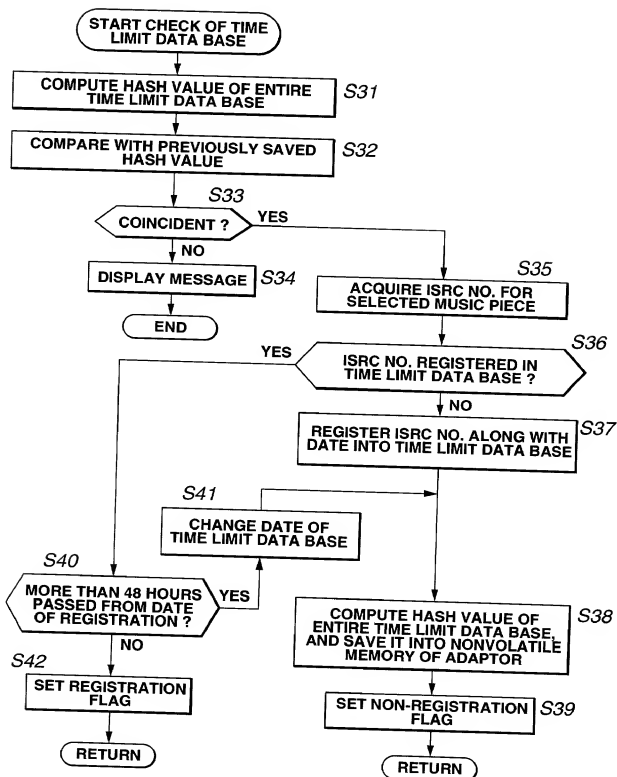


FIG.8

9/36

## TIME LIMIT DATA BASE

	ITEM 1	ITEM 2	ITEM 3	
ISRC	JP-Z90-98-12345	US-Z90-99-12346	JP-Z90-98-12347	
DATE OF COPY	1998.11.23.08:04	2004.03.06.16:09	2004.03.06.16.15	

HASH VALUE	0xf3352e125934
---------------	----------------

FIG.9

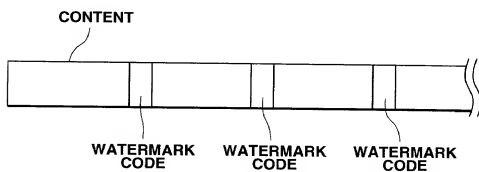


FIG.10

## MUSIC DATA BASE

	ITEM 1	ITEM 2	ITEM 3	
FILE NAME	Xd000110. at2	px92341234. at2	aa0234287034. at2	
ENCRYPTED ENCRYPTION KEY	0xabababababab	0x9898989898989	0x123456789012	
MUSIC PIECE NAME	HARU-NO-OGAWA	UNMEI(DESTINY)	KOUJOU-NO-TSUKI	
PLAY TIME LENGTH	180	190	200	
PLAYBACK CONDITION : START DATE	-	2001.01.01.00:00	-	
PLAYBACK CONDITION : END DATE	1999.07.31.23:59	-	-	
PLAYBACK CONDITION : PLAYBACK LIMIT	-	20	-	
PLAYBACK COUNTER	-	12	-	
PLAYBACK ACCOUNTING CONDITION	-	-	¥5	
COPYING CONDITION : COPIES	2	0	0	
COPY COUNTER	1	0	0	
COPYING CONDITION : SCMS	0b01	0b10	0b00	

HASH VALUE	0xf9951e566321
------------	----------------

FIG.11

11/36

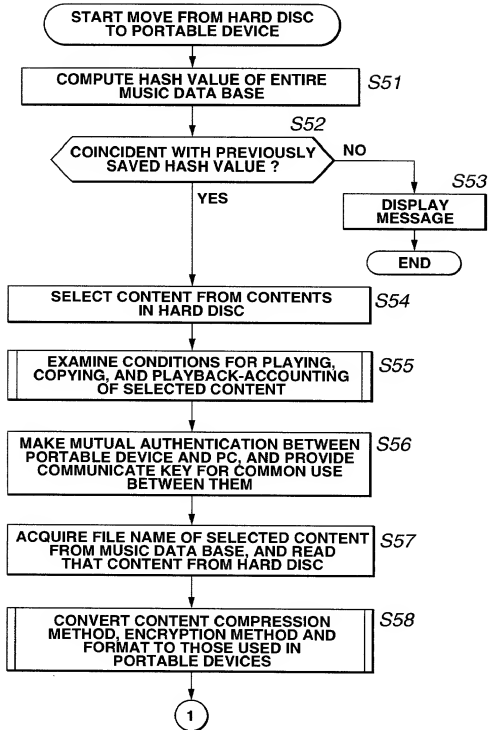


FIG.12

12/36

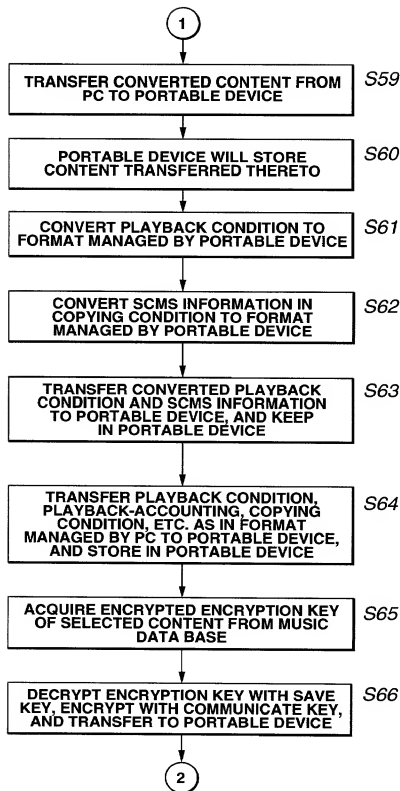


FIG.13

13/36

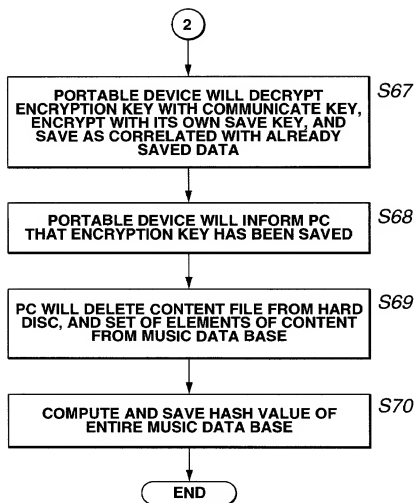


FIG.14

14/36

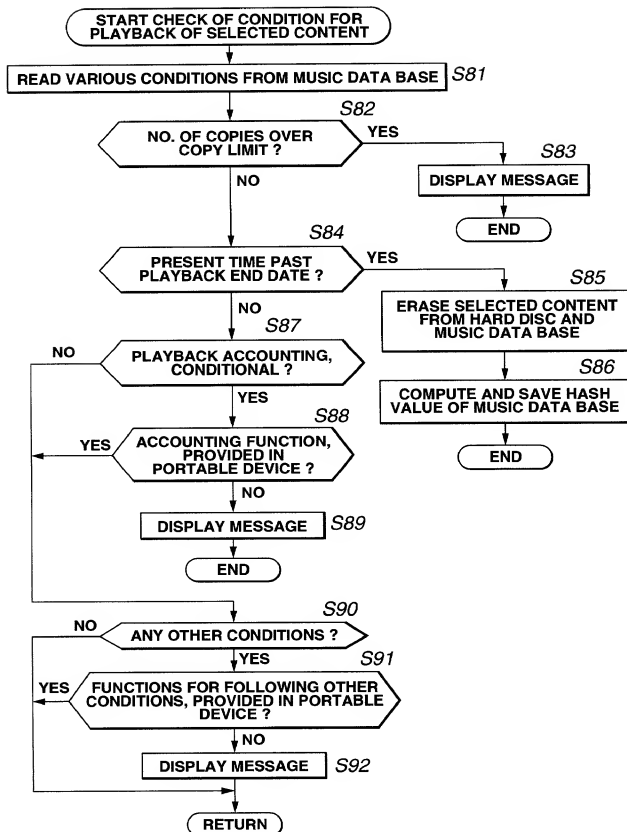


FIG.15



**PLAYBACK CONDITIONS MANAGED BY PORTABLE DEVICE**

	ITEM 1	ITEM 2	ITEM 3
<b>CONTENT ID</b>	00001	00002	00003
<b>PLAY START DATE</b>	1999.07.31.23:59	1999.07.31.23:59	1999.07.31.23:59
<b>PLAY END DATE</b>	2001.01.01.00:00	2001.01.01.00:00	2001.01.01.00:00
<b>PLAYBACK LIMIT</b>	-	15	-

**FIG.16**

16/36

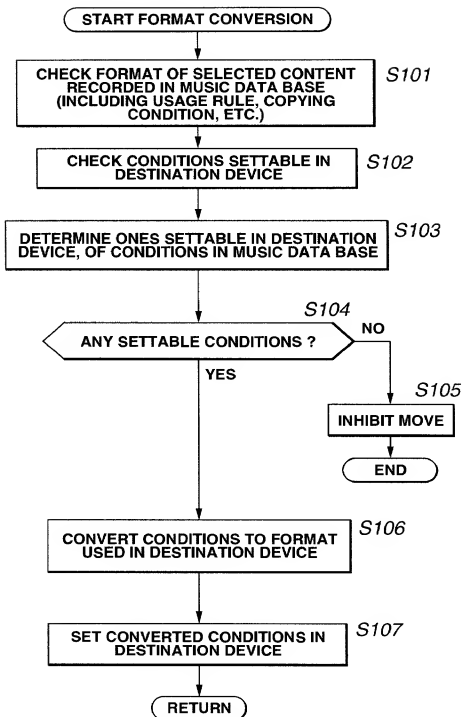


FIG.17

17/36

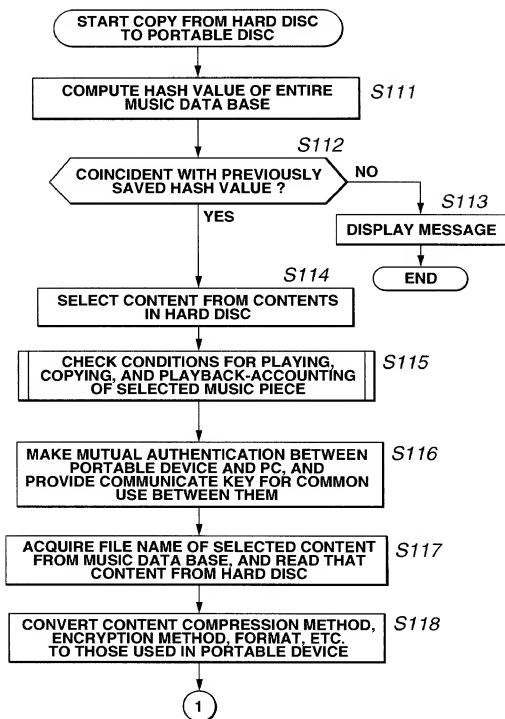


FIG.18

18/36

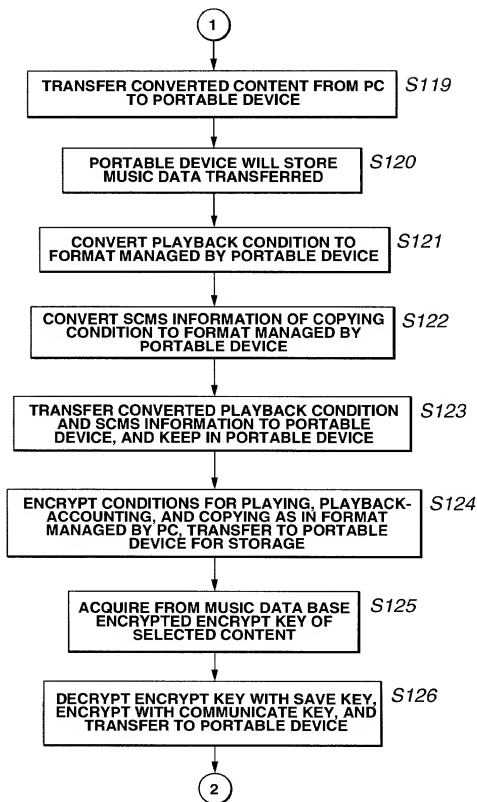


FIG.19

19/36

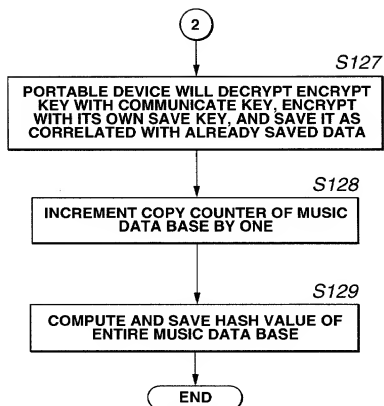


FIG.20

20/36

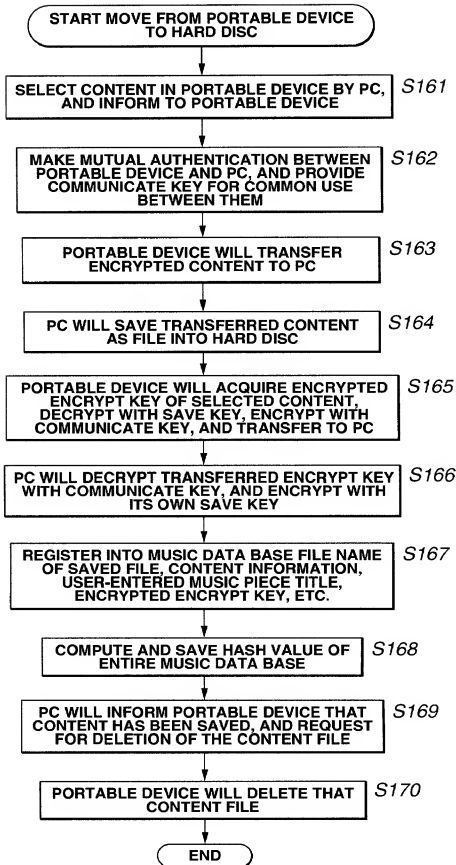


FIG.21

21/36

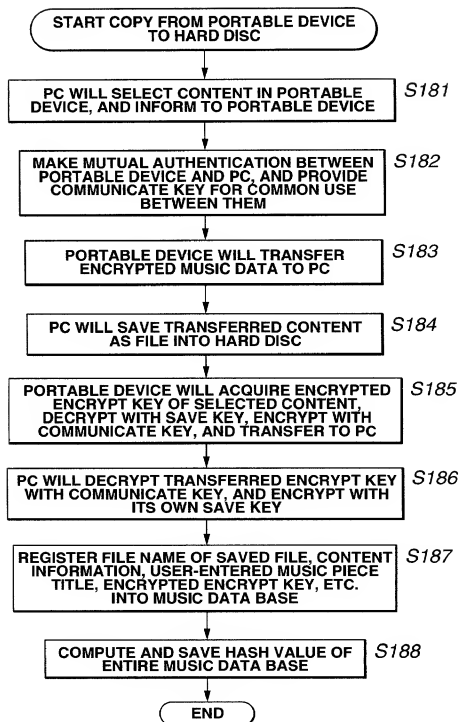


FIG.22

22/36

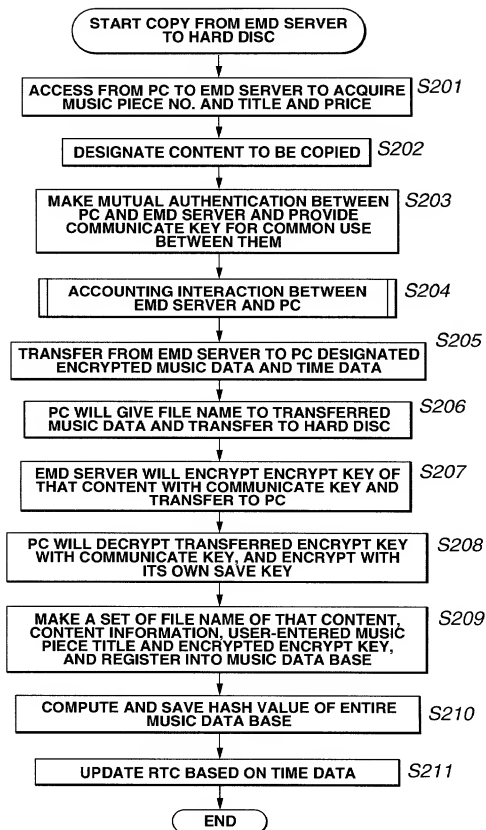


FIG.23



23/36

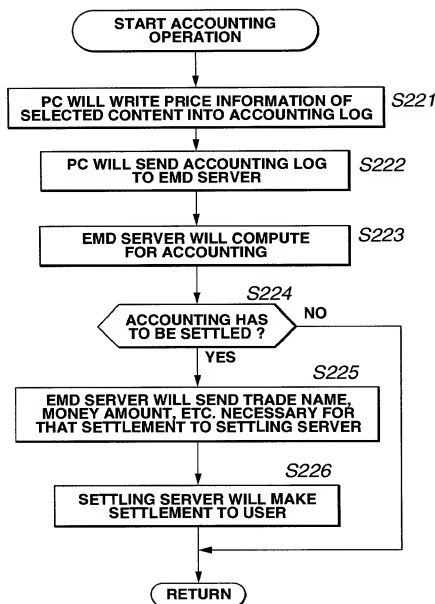


FIG.24

24/36

**ACCOUNTING LOG**

	ITEM 1	ITEM 2	ITEM 3	
FEE	50	50	60	

HASH VALUE	0xf8783e263517
------------	----------------

**FIG.25**

25/36

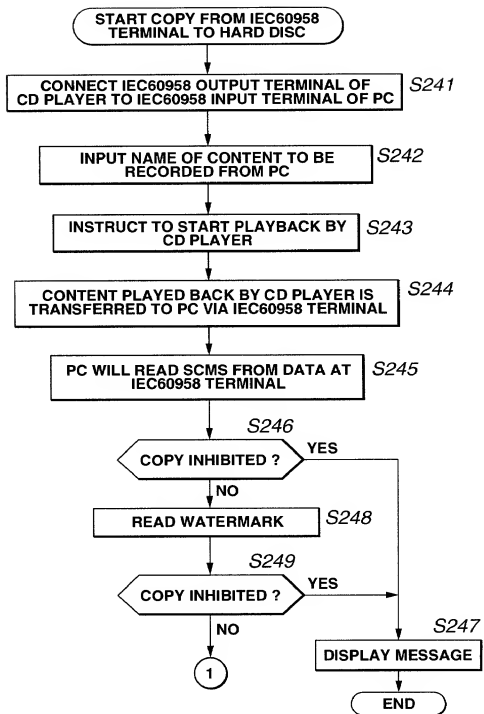


FIG.26

26/36

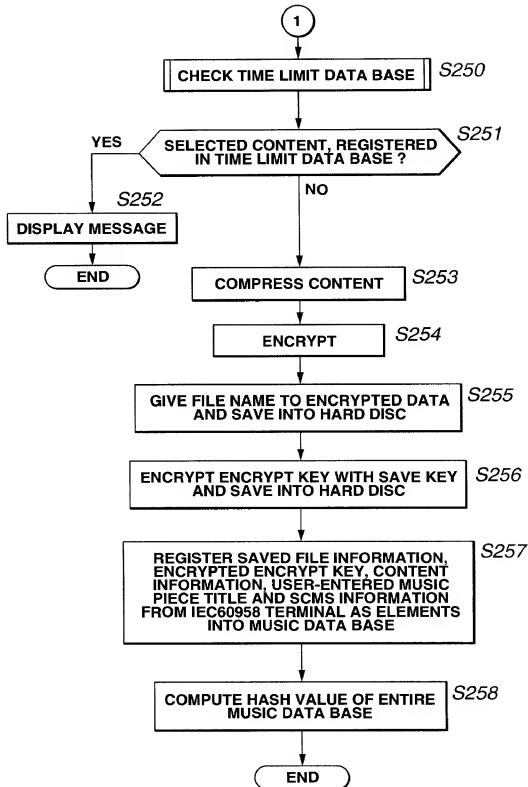


FIG.27

27/36

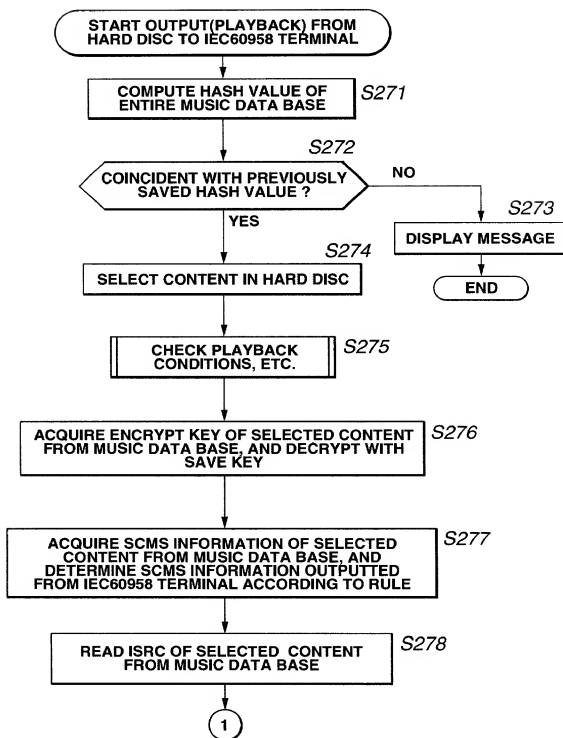


FIG.28

28/36

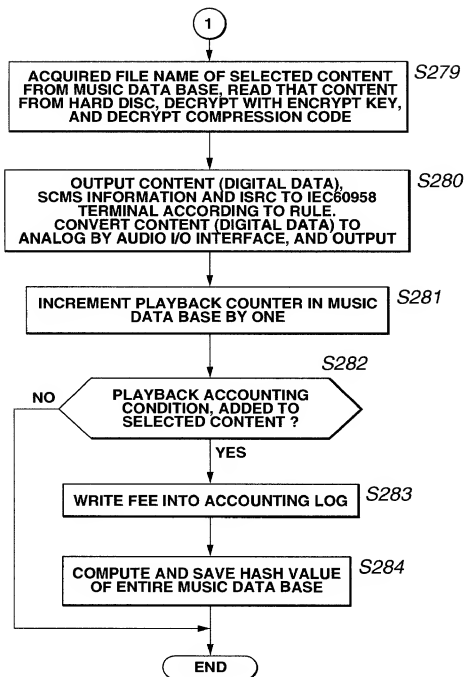


FIG.29

29/36

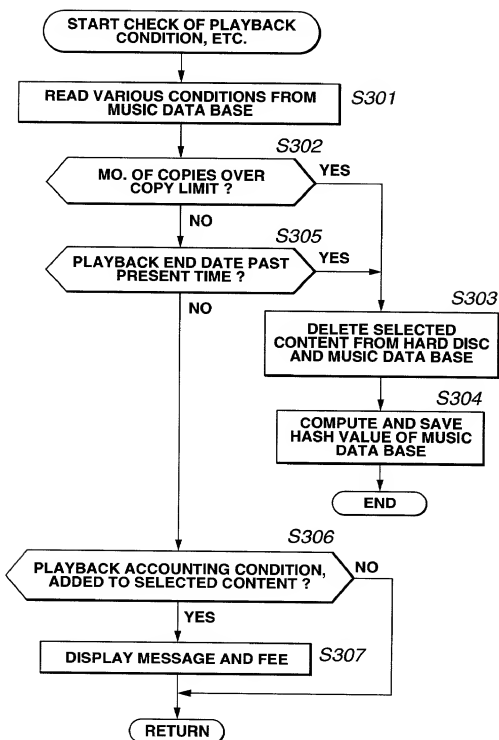


FIG.30

30/36

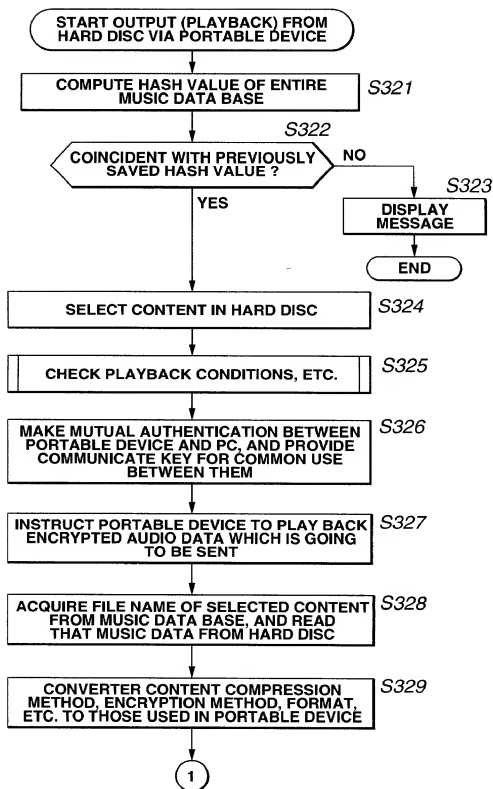


FIG.31



31/36

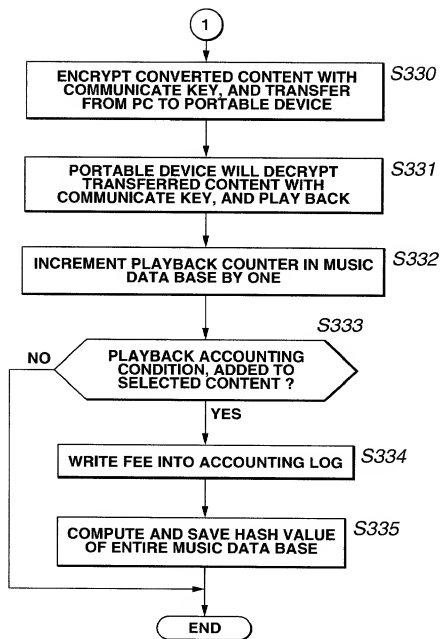


FIG.32

32/36

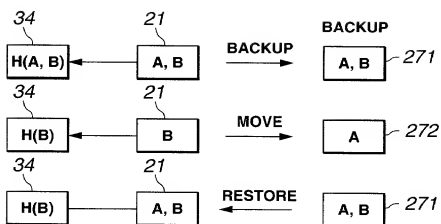


FIG.33

33/36

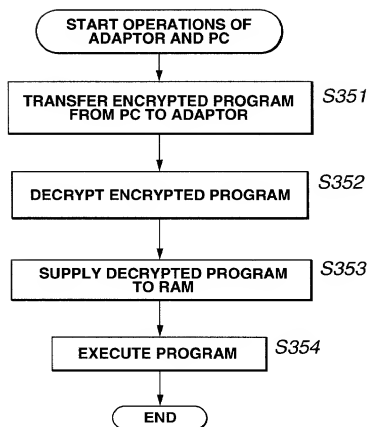


FIG.34

34/36

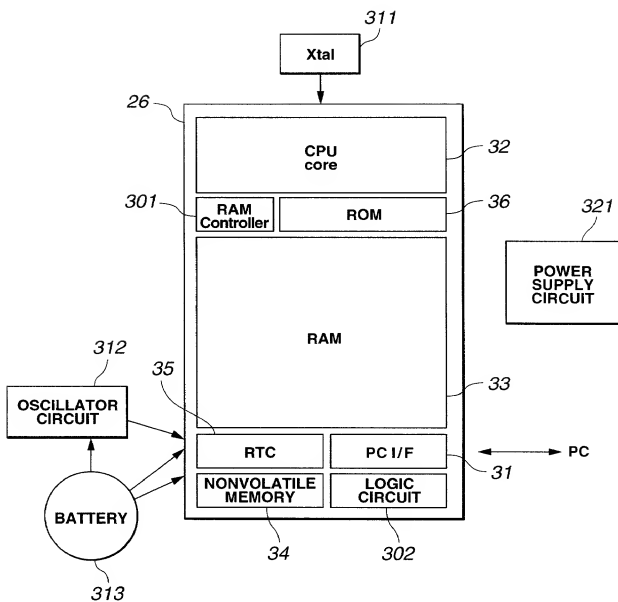
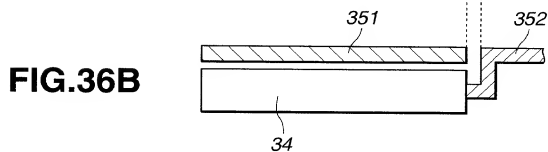
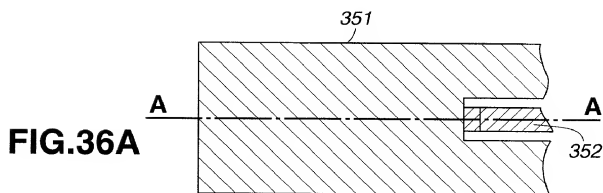
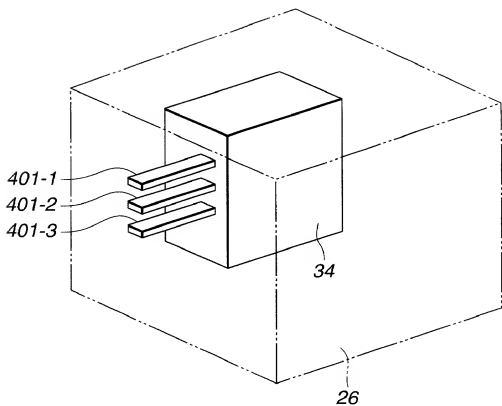


FIG.35

35/36



36/36

**FIG. 37**

Atty Docket No. KOIK-T0185**COMBINED DECLARATION FOR PATENT APPLICATION AND POWER OF ATTORNEY**

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name,

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled

INFORMATION PROCESSING APPARATUS AND METHOD, AND PROGRAM STORAGE MEDIUM

the specification of which (check one)    is attached hereto or X was filed on February 17, 2000 (International Filing Date) as International Application no. PCT/JP00/00904 and was amended on    (if applicable).

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose all information which is material to patentability as defined in 37 CFR § 1.56.

I hereby claim foreign priority benefits under 35 U.S.C. § 119(a)-(d) or § 365(b) of any foreign application(s) for patent or inventor's certificate, or § 365(a) of any PCT International application which designated at least one country other than the United States, listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

Prior Foreign Application(s)			Priority Claimed	
			Yes	No
P11-039218	Japan	17 February 1999	X	
Number	Country	Day/Month/Year Filed		
PCT/JP00/00904	PCT	17 February 2000	X	
Number	Country	Day/Month/Year Filed		

I hereby claim the benefit under 35 U.S.C. § 119(e) of any United States provisional application(s) below.

Application Number	Filing Date
--------------------	-------------

Application Number	Filing Date
--------------------	-------------

I hereby claim the benefit under 35 U.S.C. § 120 of any United States application(s), or § 365(c) of any PCT International application designating the United States, listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of 35 U.S.C. § 112, I acknowledge the duty to disclose all information which is material to patentability as defined in 37 CFR § 1.56 which became available between the filing date of the prior application and the national or PCT international filing date of this application:

Application Number	Filing Date	Status: Patented, Pending, Abandoned
--------------------	-------------	--------------------------------------

Application Number	Filing Date	Status: Patented, Pending, Abandoned
--------------------	-------------	--------------------------------------

I HEREBY APPOINT THE FOLLOWING AS MY ATTORNEYS WITH FULL POWER OF SUBSTITUTION TO PROSECUTE THIS APPLICATION AND TRANSACT ALL BUSINESS IN THE PATENT OFFICE CONNECTED THEREWITH:

Karl A. Limbach	<u>18,669</u>	Mark A. Dalla Valle	<u>34,147</u>	Kyla L. Harriel	<u>41,816</u>
George C. Limbach	<u>19,306</u>	Charles P. Sammut	<u>28,801</u>	Mayumi Maeda	<u>40,075</u>
John K. Ulkema	<u>20,282</u>	Mark C. Pickering	<u>36,239</u>	Kent J. Tobin	<u>39,496</u>
Neil A. Smith	<u>25,441</u>	Patricia Coleman James	<u>37,155</u>	Michael R. Ward	<u>38,851</u>
Veronica C. Devitt	<u>29,375</u>	Kathleen A. Frost	<u>37,326</u>	Roger S. Sampson	<u>44,314</u>
Ronald L. Yin	<u>27,607</u>	Alan S. Hodes	<u>38,185</u>	Tina Chen	<u>P.44,606</u>
Gerald T. Sekimura	<u>30,103</u>	Alan A. Limbach	<u>39,748</u>	Charles L. Hamilton	<u>42,624</u>
Michael A. Stallman	<u>29,444</u>	Douglas C. Limbach	<u>35,248</u>	Andrew V. Smith	<u>43,132</u>
Philip A. Girard	<u>28,545</u>	Brian J. Keating	<u>39,520</u>	Heath W. Hoglund	<u>41,078</u>
Michael J. Pollock	<u>23,088</u>	Seong-Kun Oh*	<u>41,897</u>	William G. Goldman	<u>42,590</u>
Stephen M. Everett	<u>30,050</u>	Cameron A. King		J. Thomas McCarthy	<u>22,420</u>
Alfred A. Equitz	<u>30,922</u>			Joel G. Ackerman	<u>24,307</u>

\* Recognition under 37 CFR 10.8(b)

34

Send correspondence to:

Limbach & Limbach L.L.P.  
2001 Ferry Building  
San Francisco, CA 94111  
Telephone: 415/433-4150

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment or both, under 18 U.S.C. § 1001 and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Full name of sole or first inventor ITARU KAWAKAMI

Inventor's signature Itaru Kawakami

Date September 25, 2000

Residence Kanagawa, Japan

Citizenship Japan

Post Office Address c/o SONY CORPORATION, 7-35, Kitashinagawa 6-chome, Shinagawa-ku, Tokyo 141-0001 Japan

Full name of second joint inventor, if any, RYUJI ISHIGURO

Inventor's signature Ryuji Ishiguro

Date September 26, 2000

Residence Tokyo, Japan

Citizenship Japan

Post Office Address c/o SONY CORPORATION, 7-35, Kitashinagawa 6-chome, Shinagawa-ku, Tokyo 141-0001 Japan

Full name of third joint inventor, if any, MITSURU TANABE

Inventor's signature Mitsuru Tanabe

Date September 25, 2000

Residence Kanagawa, Japan

Citizenship Japan

Post Office Address c/o SONY CORPORATION, 7-35, Kitashinagawa 6-chome, Shinagawa-ku, Tokyo 141-0001 Japan



Full name of fourth joint inventor, if any, YUICHI EZURA

Inventor's signature

Yuichi Ezura

September 25, 2000

Date

Residence Kanagawa, Japan

Citizenship Japan

Post Office Address c/o SONY CORPORATION, 7-35, Kitashinagawa 6-chome, Shinagawa-ku, Tokyo 141-0001 Japan